General Properties of Quantum Zero-Knowledge Proofs

Hirotada Kobayashi
hirotada@nii.ac.jp

Principles of Informatics Research Division
National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

8 May 2007

Abstract

This paper studies the complexity classes QZK and HVQZK, the classes of problems having a quantum computational zero-knowledge proof system and an *honest-verifier* quantum computational zero-knowledge proof system, respectively. The results proved in this paper include:

- HVQZK = QZK.

- Any problem in QZK has a *public-coin* quantum computational zero-knowledge proof system.

- Any problem in QZK has a quantum computational zero-knowledge proof system of *perfect completeness*.

- Any problem in QZK has a *three-message public-coin* quantum computational zero-knowledge proof system of perfect completeness with polynomially small error in soundness (hence with arbitrarily small constant error in soundness).

All the results proved in this paper are unconditional, i.e., they do not rely any computational assumptions such as the existence of quantum one-way functions or permutations. For the classes QPZK, HVQPZK, and QSZK of problems having a quantum perfect zero-knowledge proof system, an honest-verifier quantum perfect zero-knowledge proof system, and a quantum statistical zero-knowledge proof system, respectively, the following new properties are proved:

- HVQPZK = QPZK.

- Any problem in QPZK has a *public-coin* quantum perfect zero-knowledge proof system.

- Any problem in QSZK has a quantum statistical zero-knowledge proof system of *perfect completeness*.

- Any problem in QSZK has a *three-message public-coin* quantum statistical zero-knowledge proof system of perfect completeness with polynomially small error in soundness (hence with arbitrarily small constant error in soundness).

It is stressed that the proofs for all the statements are direct and do not use complete promise problems or those equivalents. This gives a *unified framework* that works well for all of quantum perfect, statistical, and computational zero-knowledge proofs. In particular, this enables us to prove properties even on the computational and perfect zero-knowledge proofs for which no complete promise problems nor those equivalents are known.

1 Introduction

1.1 Background

Zero-knowledge proof systems were introduced by Goldwasser, Micali, and Rackoff [15], and have played a central role in modern cryptography since then. Intuitively, an interactive proof system is zero-knowledge if *any* verifier who communicates with the *honest* prover learns nothing except for the validity of the statement being proved in that system. By "learns nothing" we mean that there exists a polynomial-time *simulator* whose output is indistinguishable from the output of the verifier after communicating with the honest prover. Depending on the strength of this indistinguishability, several variants of zero-knowledge proofs have been investigated: *perfect* zero-knowledge in which the output of the simulator is identical to that of the verifier, *statistical* zero-knowledge in which the output of the simulator is statistically close to that of the verifier, and *computational* zero-knowledge in which the output of the simulator is indistinguishable from that of the verifier in polynomial time. The most striking result on zero-knowledge proofs would be that every problem in NP has a computational zero-knowledge proof system under certain intractability assumptions [11] like the existence of one-way functions [24, 17]. It is also known that some problems have perfect or statistical zero-knowledge proof systems. Among others, the GRAPH ISO-MORPHISM problem has a perfect zero-knowledge proof system [11], and some lattice problems have statistical zero-knowledge proof systems [10].

Another direction of studies on zero-knowledge proofs has been to prove general properties of zero-knowledge proofs. Sahai and Vadhan [28] were the first that took an approach of characterizing zero-knowledge proofs by complete promise problems. They showed that the STATISTICAL DIFFERENCE problem is complete for the class HVSZK of problems having an *honest-verifier* statistical zero-knowledge proof system. Here, the honest-verifier zero-knowledge is a weaker notion of zero-knowledge in which now zero-knowledge property holds only against the *honest* verifier who follows the specified protocol. Using this complete promise problem, they proved a number of general properties of HVSZK and simplified the proofs of several previously known results including that HVSZK is in AM [7, 2], that HVSZK is closed under complement [26], and that any problem in HVSZK has a public-coin honest-verifier statistical zero-knowledge proof system [26]. Goldreich and Vadhan [14] presented another complete promise problem for HVSZK, called the ENTROPY DIFFERENCE problem, and obtained further properties of HVSZK. Since Goldreich, Sahai, and Vadhan [12] proved that HVSZK = SZK, where SZK denotes the class of problems having a statistical zero-knowledge proof system, all the properties for HVSZK are inherited to SZK (except for those related to round complexity). Along this line, Goldreich, Sahai, and Vadhan [13] gave two complete promise problems for the class NISZK of problems having a non-interactive statistical zero-knowledge proof system, and derived several properties of NISZK. More recently, Vadhan [31] gave two characterizations, the INDISTINGUISHABILITY characterization and the CONDITIONAL PSEUDO-ENTROPY characterization, for the class ZK of problems having a computational zero-knowledge proof system. These are not complete promise problems, but more or less analogous to complete promise problems and play essentially same roles as complete promise problems in his proof. Using these characterizations, Vadhan proved a number of general properties for ZK unconditionally (i.e., not assuming any intractability assumptions), such as that honest-verifier computational zero-knowledge equals general computational zero-knowledge, that public-coin computational zero-knowledge equals general computational zero-knowledge, and that computational zero-knowledge of perfect completeness equals general two-sided bounded error computational zero-knowledge.

Quantum zero-knowledge proofs were first studied by Watrous [32] in a restricted situation of *honest-verifier* quantum statistical zero-knowledge proofs. He gave an analogous characterization to the classical case by Sahai and Vadhan [28] by showing that the QUANTUM STATE DISTINGUISHABILITY problem is complete for the class HVQSZK of problems having an honest-verifier quantum statistical zero-knowledge proof system. Using this, he proved a number of general properties for HVQSZK, such as that HVQSZK is closed under complement, that any problem in HVQSZK has a public-coin honest-verifier quantum statistical zero-knowledge proof system, and that HVQSZK is in PSPACE. Very recently, Ben-Aroya and Ta-Shma [3] presented another complete promise

problem for HVQSZK, called the QUANTUM ENTROPY DIFFERENCE problem, which is a quantum analogue of the result by Goldreich and Vadhan [14]. Kobayashi [21] studied non-interactive quantum perfect and statistical zero-knowledge proofs again using a complete promise problem, which can be viewed as a quantum version of the classical result by Goldreich, Sahai, and Vadhan [13]. It has been a wide open problem if there are nontrivial problems that has a quantum zero-knowledge proof system secure even against any dishonest quantum verifiers, because of the difficulties arising from the "rewinding" technique [16], which is commonly-used in classical zero-knowledge proofs. Damgård, Fehr, and Salvail [5] studied zero-knowledge proofs against dishonest quantum verifier, but they assumed the restricted setting of the common-reference-string model to avoid this rewinding problem. Very recently, Watrous [34] settled this affirmatively. He developed a quantum "rewinding" technique by using a method that was originally developed in Ref. [23] for the purpose of amplifying the success probability of QMA, a quantum version of NP, without increasing quantum witness sizes. With this quantum rewinding technique, he proved that the classical protocol for the GRAPH ISOMORPHISM problem in Ref. [11] has a perfect zero-knowledge property even against any dishonest *quantum* verifiers, and under some reasonable intractability assumption, the classical protocol for NP in Ref. [11] has a computational zero-knowledge property even against any dishonest *quantum* verifiers. He also proved that HVQSZK = QSZK, where QSZK denotes the class of problems having a quantum statistical zero-knowledge proof system. This implies that all the properties for HVQSZK proved in Ref. [32] are inherited to QSZK (except for those related to round complexity), in particular, that any problem in QSZK has a public-coin quantum statistical zero-knowledge proof system.

1.2 Our Contribution

This paper proves a number of general properties on quantum zero-knowledge proofs, not restricted to quantum statistical zero-knowledge proofs. Specifically, for quantum computational zero-knowledge proofs, letting QZK and HVQZK denote the classes of problems having a quantum computational zero-knowledge proof system and an *honest-verifier* quantum computational zero-knowledge proof system, respectively, the following are proved among others:

Theorem (Theorem 29). HVQZK = QZK.

Theorem (Theorem 30). *Any problem in* QZK *has a public-coin quantum computational zero-knowledge proof system.*

Theorem (Theorem 32). *Any problem in* QZK *has a quantum computational zero-knowledge proof system of perfect completeness.*

Theorem (Theorem 34). *Any problem in* QZK *has a three-message public-coin quantum computational zero-knowledge proof system of perfect completeness with soundness error probability at most* $\frac{1}{p}$ *for any polynomially bounded function* $p\colon \mathbb{Z}^+ \to \mathbb{N}$ *(hence with arbitrarily small constant error in soundness).*

All the properties proved in this paper on quantum computational zero-knowledge proofs hold unconditionally, meaning that they hold without any computational assumptions such as the existence of quantum one-way functions or permutations. Some of these properties may be regarded as quantum versions of the results by Vadhan [31]. It is stressed, however, that our approach to prove these properties is completely different from those the existing studies took to prove general properties of classical or quantum zero-knowledge proofs. No complete promise problems nor those equivalents are used in our proofs. Instead, we *directly* prove these properties, which gives a *unified framework* that works well for all of quantum perfect, statistical, and computational zero-knowledge proofs.

The idea is remarkably simple. We start from any protocol of *honest-verifier* quantum zero-knowledge, and apply several modifications so that we finally obtain another protocol of honest-verifier quantum zero-knowledge that possesses a number of desirable properties. For instance, to prove that HVQZK = QZK, we show that any protocol of honest-verifier quantum computational zero-knowledge can be modified to another protocol of honest-verifier

quantum computational zero-knowledge (with some smaller gap between completeness and soundness accepting probabilities) such that (i) the protocol consists of three messages and (ii) the protocol is public-coin in which the message from the honest verifier consists of a single bit that is an outcome of a classical fair coin-flipping. Note that such modifications are possible in the case of usual quantum interactive proofs [20, 23], and we show that this is also the case for *honest-verifier* quantum computational zero-knowledge proofs. Now we apply the quantum rewinding technique due to Watrous [34] to show that the protocol is zero-knowledge even against any *dishonest* quantum verifiers. The final tip is the sequential repetition, which reduces completeness and soundness errors arbitrarily small. This simultaneously shows the equivalence of public-coin quantum computational zero-knowledge and general quantum computational zero-knowledge. To show that any quantum computational zero-knowledge proofs can be made perfect complete, now we have only to show that any *honest-verifier* quantum computational zero-knowledge proofs can be made perfect complete. Again a similar property is known to hold for usual quantum interactive proofs [20], and we carefully modify the protocol so that it holds even for the honest-verifier quantum computational zero-knowledge case. Using this modification as a preprocessing, the previous argument shows the equivalence of quantum computational zero-knowledge of perfect completeness and general quantum computational zero-knowledge. Combining all the desirable properties of honest-verifier quantum computational zero-knowledge proofs shown in this paper with a careful application of the quantum rewinding technique, we can show that any problem in QZK has a three-message public-coin quantum computational zero-knowledge proof system of perfect completeness with soundness error at most $\frac{1}{p}$ for any polynomially bounded function p.

In fact, our approach above is very general and basically works well even for quantum perfect and statistical zero-knowledge proofs. In the quantum statistical zero-knowledge case, all the properties shown for the quantum computational zero-knowledge case also hold. This gives alternative proofs of some of the properties obtained in Refs. [32, 34], and also shows the following new properties of quantum statistical zero-knowledge proofs:

Theorem (Theorem 37). *Any problem in* QSZK *has a quantum statistical zero-knowledge proof system of perfect completeness.*

Theorem (Theorem 38). *Any problem in* QSZK *has a three-message public-coin quantum statistical zero-knowledge proof system of perfect completeness with soundness error probability at most $\frac{1}{p}$ for any polynomially bounded function $p \colon \mathbb{Z}^+ \to \mathbb{N}$ (hence with arbitrarily small constant error in soundness).*

In the quantum perfect zero-knowledge case, however, not all the properties above can be shown to hold, because very subtle points easily lose the *perfect* zero-knowledge property. In particular, our method of making protocols perfect complete that works well for quantum computational and statistical zero-knowledge cases no longer works well for quantum perfect zero-knowledge case. Also, we need a very careful modification of the protocol when parallelizing to three messages. Still, we can show the following properties:

Theorem (Theorem 22). HVQPZK = QPZK.

Theorem (Theorem 23). *Any problem in* QPZK *has a public-coin quantum perfect zero-knowledge proof system.*

Note that no such general properties are known for the classical perfect zero-knowledge case. As a bonus property, it is also proved that the quantum perfect zero-knowledge with a worst-case polynomial-time simulator that is not allowed to output "FAIL" is equivalent to the one in which a simulator is allowed to output "FAIL" with small probability. Again, such equivalence is not known in the classical case.

1.3 Organization of This Paper

This paper is organized as follows. Section 2 summarizes the notions and notations that are used in this paper. Sections 3, 4, and 5 treat our results for quantum perfect, computational, and statistical zero-knowledge proofs, respectively. In order to present a unified framework that works well for all of quantum perfect, computational,

and statistical zero-knowledge proofs, we first show the results for the perfect zero-knowledge case. This may involve more careful modifications of the protocols that are necessary only for the perfect zero-knowledge case, but once we have presented how to modify the protocols, we can avoid complications arising from imperfect zero-knowledge conditions when proving zero-knowledge property, which will be helpful to illustrate most of our proof structures in a simpler setting. Section 6 proves the equivalence of two different definitions of quantum perfect zero-knowledge. Finally, Section 7 concludes the paper with some open problems.

2 Preliminaries

We assume the reader is familiar with classical zero-knowledge proof systems and quantum interactive proof systems. Detailed discussions of classical zero-knowledge proof systems can be found in Refs. [8, 9], for instance, while quantum interactive proof systems are discussed in Refs. [33, 20, 23] and are reviewed in Appendix A. We also assume familiarity with the quantum formalism, including the quantum circuit model and definitions of mixed quantum states, admissible transformations (completely-positive trace-preserving mappings), trace norm, diamond norm, and fidelity (all of which are discussed in detail in Refs. [25, 19], for instance).

Some of the notions and notations that are used in this paper are summarized in this section.

Throughout this paper, let $\mathbb{N}$ and $\mathbb{Z}^+$ denote the sets of positive and nonnegative integers, respectively. For every $d \in \mathbb{N}$, let I_d denote the identity operator of dimension d. Also, for any Hilbert space $\mathcal{H}$, let $I_{\mathcal{H}}$ denote the identity operator over $\mathcal{H}$. In this paper, all Hilbert spaces are of dimension power of two.

2.1 Quantum Formalism

For any Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, let $\mathbf{D}(\mathcal{H})$, $\mathbf{U}(\mathcal{H})$, and $\mathbf{T}(\mathcal{H}, \mathcal{K})$ denote the sets of density operators over $\mathcal{H}$, unitary operators over $\mathcal{H}$, and admissible transformations from $\mathcal{H}$ to $\mathcal{K}$, respectively. For any Hilbert space $\mathcal{H}$, let $|0_{\mathcal{H}}\rangle$ denote the quantum state in $\mathcal{H}$ of which all the qubits are in state $|0\rangle$.

Let $\mathcal{H}$ and $\mathcal{K}$ be the Hilbert spaces and let $\Phi \in \mathbf{T}(\mathcal{H}, \mathcal{K})$ be an admissible transformation. Let $\mathcal{N}$, $\mathcal{X}$, and $\mathcal{Y}$ be Hilbert spaces such that $\mathcal{H} \otimes \mathcal{X} = \mathcal{K} \otimes \mathcal{Y} = \mathcal{N}$. A unitary transformation $U_\Phi \in \mathbf{U}(\mathcal{N})$ is a *unitary realization* of Φ if $\mathrm{tr}_{\mathcal{Y}} U_\Phi (\rho \otimes |0_{\mathcal{X}}\rangle\langle 0_{\mathcal{X}}|) U_\Phi^\dagger = \Phi(\rho)$ for any $\rho \in \mathbf{D}(\mathcal{H})$.

The following approximate version of unitary equivalence is used in this paper.

Lemma 1 ([32]). *For Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, let $|\phi\rangle, |\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ satisfy that $F(\mathrm{tr}_{\mathcal{K}} |\phi\rangle\langle\phi|, \mathrm{tr}_{\mathcal{K}} |\psi\rangle\langle\psi|) \geq 1 - \varepsilon$ for some $\varepsilon \in [0, 1]$. Then there exists a unitary transformation $U \in \mathbf{U}(\mathcal{K})$ such that $\|(I_{\mathcal{H}} \otimes U)|\phi\rangle - |\psi\rangle\| \leq \sqrt{2\varepsilon}$.*

2.2 Quantum Circuits and Polynomial-Time Preparable Ensembles of Quantum States

It is assumed that any quantum circuit Q in this paper is unitary and is composed of gates in some reasonable, universal, finite set of unitary quantum gates. For convenience, we may identify a circuit Q with the unitary operator it induces.

Since non-unitary and unitary quantum circuits are equivalent in computational power [1], it is sufficient to treat only unitary quantum circuits, which justifies the above assumption. For avoiding unnecessary complication, however, the descriptions of procedures often include non-unitary operations in the subsequent sections. Even in such cases, it is always possible to construct unitary quantum circuits that essentially achieve the same procedures described. A quantum circuit Q is q_{in}-*in* q_{out}-*out* if it exactly implements a unitary realization U_Φ of some q_{in}-in q_{out}-out admissible transformation Φ. For convenience, we may identify a circuit Q with Φ in such a case. As a special case of this, a quantum circuit Q is a *generating circuit* of a quantum state ρ of q qubits if it exactly implements a unitary realization of a zero-in q-out admissible transformation that always outputs ρ.

Following preceding studies on quantum interactive and zero-knowledge proofs, this paper uses the following notion of polynomial-time uniformly generated families of quantum circuits.

A family $\{Q_x\}$ of quantum circuits is *polynomial-time uniformly generated* if there exists a deterministic procedure that, on every input x, outputs a description of Q_x and runs in time polynomial in $|x|$. It is assumed that the number of gates in any circuit is not more than the length of the description of that circuit. Hence Q_x must have size polynomial in $|x|$.

When proving statements concerning quantum perfect zero-knowledge proofs or proofs having perfect completeness, we assume that our universal gate set satisfies some conditions, since these "perfect" properties may not hold with an arbitrary universal gate set. In fact, this is also the case for some previous studies on quantum interactive or zero-knowledge proofs, including the papers by Kitaev and Watrous [20] and by Marriott and Watrous [23], when deriving statements with perfect completeness property. The correctness of our results concerning quantum perfect zero-knowledge proofs or proofs having perfect completeness may be discussed under a similar assumption to those studies on the choice of the universal gate set. Fortunately, the author learned from John Watrous [35] that the choice of the gate set would not be so critical and all the "perfect" properties claimed in Refs. [20, 23] and in this paper hold with any gate set such that the Hadamard transformation and any classical reversible transformations are exactly implementable. Note that this condition is satisfied by most of the standard gate sets including the Shor basis [30] consisting of the Hadamard gate, the controlled-i-phase-shift gate, and the Toffoli gate. These subtle issues regarding choices of the universal gate set will be explained in detail in Appendix B. It is stressed, however, that all of our statements not concerning quantum perfect zero-knowledge proofs nor proofs having perfect completeness do hold for an arbitrary choice of the universal gate set (the completeness and soundness conditions may become worse by negligible amounts in some of the claims, which does not matter for the final main statements).

Finally, this paper uses the following notion of polynomial-time preparable ensembles of quantum states, which was introduced in Ref. [32].

An ensemble $\{\rho_x\}$ of quantum states is *polynomial-time preparable* if there exists a polynomial-time uniformly generated family $\{Q_x\}$ of quantum circuits such that each Q_x is a generating circuit of ρ_x. In what follows, we may use the notation $\{\rho(x)\}$ instead of $\{\rho_x\}$ for ensembles of quantum states simply for descriptional convenience.

2.3 Quantum Computational Indistinguishability

We use the notions of quantum computational indistinguishability introduced by Watrous [34]: polynomially quantum indistinguishable ensembles of quantum states and polynomially quantum indistinguishable ensembles of admissible transformations.

First, the quantum computational indistinguishability between two ensembles of quantum states is defined as follows.

Definition 2. Let $S \subseteq \{0, 1\}^*$ be an infinite set and let $m \colon \mathbb{Z}^+ \to \mathbb{N}$ be a polynomially bounded function. For each $x \in S$, let ρ_x and σ_x be mixed states of $m(|x|)$ qubits. The ensembles $\{\rho_x \colon x \in S\}$ and $\{\sigma_x \colon x \in S\}$ are *polynomially quantum indistinguishable* if, for every choice of

- polynomially bounded functions $k, p, s \colon \mathbb{Z}^+ \to \mathbb{N}$,

- an ensemble $\{\xi_x \colon x \in S\}$, where ξ_x is a mixed state of $k(|x|)$ qubits, and

- an $(m(|x|) + k(|x|))$-in 1-out quantum circuit Q of size at most $s(|x|)$,

it holds that

$$|\langle 1|Q(\rho_x \otimes \xi_x)|1\rangle - \langle 1|Q(\sigma_x \otimes \xi_x)|1\rangle| < \frac{1}{p(|x|)}$$

for all but finitely many $x \in S$.

Next, the quantum computational indistinguishability between two ensembles of admissible transformations is defined as follows.

Definition 3. Let $S \subseteq \{0,1\}^*$ be an infinite set and let $l, m \colon \mathbb{Z}^+ \to \mathbb{N}$ be polynomially bounded functions. For each $x \in S$, let Φ_x and Ψ_x be $l(|x|)$-in $m(|x|)$-out admissible transformations. The ensembles $\{\Phi_x \colon x \in S\}$ and $\{\Psi_x \colon x \in S\}$ are *polynomially quantum indistinguishable* if, for every choice of

- polynomially bounded functions $k, p, s \colon \mathbb{Z}^+ \to \mathbb{N}$,

- an ensemble $\{\xi_x \colon x \in S\}$, where ξ_x is a mixed state of $l(|x|) + k(|x|)$ qubits, and

- an $(m(|x|) + k(|x|))$-in 1-out quantum circuit Q of size at most $s(|x|)$,

it holds that
$$\left| \langle 1| Q\big((\Phi_x \otimes I_{2^{k(|x|)}})(\xi_x)\big)|1\rangle - \langle 1| Q\big((\Psi_x \otimes I_{2^{k(|x|)}})(\xi_x)\big)|1\rangle \right| < \frac{1}{p(|x|)}$$

for all but finitely many $x \in S$.

In what follows, we will often use the term "computationally indistinguishable" instead of "polynomially quantum indistinguishable" for simplicity. Also, we will often informally say that mixed states ρ_x and σ_x or admissible transformations Φ_x and Ψ_x are computationally indistinguishable when $x \in S$ to mean that the ensembles $\{\rho_x \colon x \in S\}$ and $\{\sigma_x \colon x \in S\}$ or $\{\Phi_x \colon x \in S\}$ and $\{\Psi_x \colon x \in S\}$ are polynomially quantum indistinguishable.

2.4 Quantum Zero-Knowledge Proofs

For readability, in what follows, the arguments x and n are dropped in the various functions, if it is not confusing. It is assumed that operators acting on subsystems of a given system are extended to the entire system by tensoring with the identity, since it will be clear from context upon what part of a system a given operator acts. Although all the statements in this paper can be proved only in terms of languages without using promise problems [6], in what follows we define models and prove statements in terms of promise problems, for generality and for the compatibility with some other studies on quantum zero-knowledge proofs [32, 21, 34, 3].

First we define the notions of various *honest-verifier* quantum zero-knowledge proofs following a manner in Ref. [32] for the statistical zero-knowledge case. Given a quantum verifier V and a quantum prover P, let $\mathrm{view}_{V,P}(x, j)$ be the quantum state that V possesses immediately after the jth transformation of P during an execution of the protocol between V and P. In other words, $\mathrm{view}_{V,P}(x, j)$ is the state obtained by tracing out the private space of P from the state of the entire system immediately after the jth transformation of P.

Now we define the classes $\mathrm{HVQPZK}(m, c, s)$, $\mathrm{HVQSZK}(m, c, s)$, and $\mathrm{HVQZK}(m, c, s)$ of problems having m-message honest-verifier quantum perfect, statistical, and computational zero-knowledge proof systems, respectively, with completeness accepting probability at least c and soundness accepting probability at most s.

Definition 4. Given a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0, 1]$, a problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ is in $\mathrm{HVQPZK}(m, c, s)$ iff there exists an m-message honest quantum verifier V and an m-message honest quantum prover P such that

(Completeness and Soundness) (V, P) forms an m-message quantum interactive proof system with completeness accepting probability at least c and soundness accepting probability at most s,

(Honest-Verifier Perfect Zero-Knowledge) there exists a polynomial-time preparable ensembles $\{S_V(x, j)\}$ of quantum states such that $S_V(x, j) = \mathrm{view}_{V,P}(x, j)$ for every $x \in A_{\mathrm{yes}}$ and for each $1 \leq j \leq \lceil \frac{m(|x|)}{2} \rceil$.

Definition 5. Given a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0,1]$, a problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in $\text{HVQSZK}(m, c, s)$ iff there exists an m-message honest quantum verifier V and an m-message honest quantum prover P such that

(Completeness and Soundness) (V, P) forms an m-message quantum interactive proof system with completeness accepting probability at least c and soundness accepting probability at most s,

(Honest-Verifier Statistical Zero-Knowledge) there exists a polynomial-time preparable ensembles $\{S_V(x, j)\}$ of quantum states such that $\|S_V(x, j) - \text{view}_{V,P}(x, j)\|_{\text{tr}}$ is negligible with respect to $|x|$ for all but finitely many $(x, j) \in A_{\text{yes}} \times \{1, \ldots, \lceil \frac{m(|x|)}{2} \rceil\}$.

Definition 6. Given a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0,1]$, a problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in $\text{HVQZK}(m, c, s)$ iff there exists an m-message honest quantum verifier V and an m-message honest quantum prover P such that

(Completeness and Soundness) (V, P) forms an m-message quantum interactive proof system with completeness accepting probability at least c and soundness accepting probability at most s,

(Honest-Verifier Computational Zero-Knowledge) there exists a polynomial-time preparable ensembles $\{S_V(x, j)\}$ of quantum states such that the ensembles $\{S_V(x, j) \colon x \in A_{\text{yes}} \text{ and } j \in \{1, \ldots, \lceil \frac{m(|x|)}{2} \rceil\}\}$ and $\{\text{view}_{V,P}(x, j) \colon x \in A_{\text{yes}} \text{ and } j \in \{1, \ldots, \lceil \frac{m(|x|)}{2} \rceil\}\}$ are polynomially quantum indistinguishable.

Remark. In the original definition of honest-verifier quantum statistical zero-knowledge by Watrous [32], the simulator is required to simulate the quantum state that V possesses immediately after the jth *message*, for every j. That is, regardless of whether the jth message is sent from P or from V, the simulator must be able to simulate the quantum state that V possesses immediately after the jth message. In our definition, the simulator is required to simulate it only when the jth message is from P. Notice, however, that every transformation of V is necessarily simulatable by the simulator, which implies that our condition is sufficient and does not weaken the honest-verifier zero-knowledge property.

Using these, we define the classes HVQPZK, HVQSZK, and HVQZK of problems having honest-verifier quantum perfect, statistical, and computational zero-knowledge proof systems, respectively.

Definition 7. A problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in HVQPZK if there exists a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ such that A is in $\text{HVQPZK}\left(m, \frac{2}{3}, \frac{1}{3}\right)$.

Definition 8. A problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in HVQSZK if there exists a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ such that A is in $\text{HVQSZK}\left(m, \frac{2}{3}, \frac{1}{3}\right)$.

Definition 9. A problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in HVQZK if there exists a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ such that A is in $\text{HVQZK}\left(m, \frac{2}{3}, \frac{1}{3}\right)$.

Note that it is easy to see that we can amplify the success probability of honest-verifier quantum perfect/statistical/computational zero-knowledge proof systems by a sequential repetition, which justifies Definitions 7, 8, and 9.

Next we define the notions of various quantum zero-knowledge proofs following a manner in Ref. [34].

Let V be an arbitrary quantum verifier. Suppose that V possesses some auxiliary quantum state in $\mathbf{D}(\mathcal{A})$ at the beginning for some Hilbert space $\mathcal{A}$, and possesses some quantum state in $\mathbf{D}(\mathcal{Z})$ after the protocol for some Hilbert space $\mathcal{Z}$. For such V, for any quantum prover P, and for every $x \in \{0,1\}^*$, let $\langle V, P \rangle(x)$ denote the admissible transformation in $\mathbf{T}(\mathcal{A}, \mathcal{Z})$ induced by the interaction between V and P on input x. We call this $\langle V, P \rangle(x)$ the *induced admissible transformation* from V, P, and x.

We define the classes $\mathrm{QPZK}(m, c, s)$, $\mathrm{QSZK}(m, c, s)$, and $\mathrm{QZK}(m, c, s)$ of problems having m-message quantum perfect, statistical, and computational zero-knowledge proof systems, respectively, with completeness accepting probability at least c and soundness accepting probability at most s, as follows.

Definition 10. Given a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0, 1]$, a problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in $\mathrm{QPZK}(m, c, s)$ iff there exists an m-message honest quantum verifier V and an m-message honest quantum prover P such that

(Completeness and Soundness) (V, P) forms an m-message quantum interactive proof system with completeness accepting probability at least c and soundness accepting probability at most s,

(Perfect Zero-Knowledge) for any m-message quantum verifier V', there exists a polynomial-time uniformly generated family $\{Q_x\}$ of quantum circuits, where each Q_x exactly implements an admissible transformation $S_{V'}(x)$, such that $S_{V'}(x) = \langle V', P \rangle(x)$ for every $x \in A_{\text{yes}}$, where $\langle V', P \rangle(x)$ is the induced admissible transformation from V', P, and x.

Definition 11. Given a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0, 1]$, a problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in $\mathrm{QSZK}(m, c, s)$ iff there exists an m-message honest quantum verifier V and an m-message honest quantum prover P such that

(Completeness and Soundness) (V, P) forms an m-message quantum interactive proof system with completeness accepting probability at least c and soundness accepting probability at most s,

(Statistical Zero-Knowledge) for any m-message quantum verifier V', there exists a polynomial-time uniformly generated family $\{Q_x\}$ of quantum circuits, where each Q_x exactly implements an admissible transformation $S_{V'}(x)$, such that $\|S_{V'}(x) - \langle V', P \rangle(x)\|_\diamond$ is negligible with respect to $|x|$ for all but finitely many $x \in A_{\text{yes}}$, where $\langle V', P \rangle(x)$ is the induced admissible transformation from V', P, and x.

Definition 12. Given a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0, 1]$, a problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in $\mathrm{QZK}(m, c, s)$ iff there exists an m-message honest quantum verifier V and an m-message honest quantum prover P such that

(Completeness and Soundness) (V, P) forms an m-message quantum interactive proof system with completeness accepting probability at least c and soundness accepting probability at most s,

(Computational Zero-Knowledge) for any m-message quantum verifier V', there exists a polynomial-time uniformly generated family $\{Q_x\}$ of quantum circuits, where each Q_x exactly implements an admissible transformation $S_{V'}(x)$, such that the ensembles $\{S_{V'}(x) \colon x \in A_{\text{yes}}\}$ and $\{\langle V', P \rangle(x) \colon x \in A_{\text{yes}}\}$ are polynomially quantum indistinguishable, where $\langle V', P \rangle(x)$ is the induced admissible transformation from V', P, and x.

Using these, we define the classes QPZK, QSZK, and QZK of problems having quantum perfect, statistical, and computational zero-knowledge proof systems, respectively.

Definition 13. A problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in QPZK if there exists a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ such that A is in $\mathrm{QPZK}\left(m, \frac{2}{3}, \frac{1}{3}\right)$.

Definition 14. A problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in QSZK if there exists a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ such that A is in $\mathrm{QSZK}\left(m, \frac{2}{3}, \frac{1}{3}\right)$.

Definition 15. A problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in QZK if there exists a polynomially bounded function $m\colon \mathbb{Z}^+ \to \mathbb{N}$ such that A is in QZK $\left(m, \frac{2}{3}, \frac{1}{3}\right)$.

Note that again it is not hard to see that we can amplify the success probability of quantum perfect/statistical/computational zero-knowledge proof systems by a sequential repetition, which justifies Definitions 13, 14, and 15.

Remark. It is noted that, in the classical case, the most common definition of perfect zero-knowledge proofs seems to allow the simulator to output "FAIL" with small probability, say, with probability at most $\frac{1}{2}$ [8, 28]. Adopting this convention leads to alternative definitions of honest-verifier and general quantum perfect zero-knowledge proof systems. At a glance, these two types of definitions seem likely to form different complexity classes of quantum perfect zero-knowledge proofs. Fortunately, it is proved from our results shown in Section 3 that it is *not* the case and the two types of definitions result in the same complexity class of quantum perfect zero-knowledge proofs. It is stressed that such equivalence is not known in the classical case. See Section 6 for further discussions on the definitions of quantum perfect zero-knowledge.

3 Perfect Zero-Knowledge Case

We first discuss the case of quantum perfect zero-knowledge proofs. This gives a unified framework that works well for all of quantum perfect, statistical, and computational zero-knowledge proofs. Although we need very careful modifications of the protocols that are necessary only for the perfect zero-knowledge case, once we have presented how to modify the protocols, we can avoid complications arising from imperfect zero-knowledge conditions when proving zero-knowledge property. Indeed, the cases of quantum computational and statistical zero-knowledge proofs are proved in almost same ways, as will be discussed later, except that we need bit more complicated arguments when proving zero-knowledge conditions.

3.1 Parallelization of Honest-Verifier Quantum Perfect Zero-Knowledge Proof Systems

This subsection proves that any honest-verifier quantum perfect zero-knowledge proof system that involves polynomially many messages can be parallelized to one that involves only three messages.

In the case of usual quantum interactive proofs, Kitaev and Watrous [20] proved the parallelizability to three messages. Here we modify their method so that it works well with honest-verifier quantum perfect zero-knowledge proofs. Actually, the method due to Kitaev and Watrous works well even in the cases of honest-verifier quantum statistical or computational zero-knowledge proofs (if the completeness error is negligible, which may be assumed without loss of generality since the success probability can be amplified by sequential repetition), and thus, we do not need our modified version in these cases. However, we do need our modified version in the case of honest-verifier quantum perfect zero-knowledge proofs, since the Kitaev-Watrous method may not preserve the *perfect* zero-knowledge property for proof systems of imperfect completeness. We explain this in more detail.

The main idea in the original parallelization protocol in Ref. [20] is that the verifier receives each snapshot state of the underlying protocol as the first message, and then checks if the following three properties are satisfied: (i) the first snapshot state is a legal state in the underlying protocol after the first message, (ii) the last snapshot state can make the original verifier accept, and (iii) any two consecutive snapshot states are indeed transformable with each other by one round of communication. In order to check these three, at the first transformation of the verifier in the original parallelization protocol in Ref. [20], he first checks if the conditions (i) and (ii) really hold for the received snapshot states, which aims to prevent a dishonest prover from preparing any illegal sequence of snapshot states that can pass the check for the condition (iii) by violating the conditions on the initial and last snapshot states. The problem arises here, in the check for the last snapshot state, when we want to parallelize a protocol of honest-verifier quantum perfect zero-knowledge with imperfect completeness. Because of imperfect completeness, the verifier's check can fail even if the honest prover prepares every snapshot state honestly, which means that the verifier's check

causes a small perturbation to the snapshot states. Now we have difficulty in *perfectly* simulating the behavior of the honest prover with respect to this perturbed state, which causes the loss of the perfect zero-knowledge property.

To avoid this difficulty, we modify the parallelization protocol as follows. Our basic idea is to postpone the verifier's check for the last snapshot state until after the third message. At the final verification of the verifier, he either carries out the postponed check for the last snapshot state with probability $\frac{1}{2}$, or just carries out the original final verification procedure with probability $\frac{1}{2}$. Now the honest-verifier perfect zero-knowledge property becomes straightforward, since there is no perturbation to all the snapshot states until after the last transformation of the verifier. The completeness property cannot become worse than that in the original protocol. However, the soundness condition now becomes a bit harder to prove, because we can no longer assume that a sequence of snapshot states prepared by a dishonest prover satisfies the condition (ii), when analyzing the probability to pass the transformability test for (iii). To overcome this, we show a general property in quantum information theory in Lemma 16, which is a generalization of Lemma 5 in Ref. [20]. This generalization enables us to analyze the case in which the last snapshot state may not necessarily make the original verifier accept, and thus, has much more flexibility than Lemma 5 in Ref. [20], which is applicable only to the case in which the last snapshot state makes the original verifier accept with certainty.

Lemma 16. *Let $\mathcal{V}$ and $\mathcal{M}$ be any Hilbert spaces. For a positive integer $k \geq 2$ and $\varepsilon, \delta \in [0,1]$ such that $\varepsilon < \delta$, suppose that a sequence of unitary operators $V_1, \ldots, V_k \in \mathbf{U}(\mathcal{V} \otimes \mathcal{M})$ and a projection operator Π acting over $\mathcal{V} \otimes \mathcal{M}$ onto some subspace of $\mathcal{V} \otimes \mathcal{M}$ satisfy that $\|\Pi V_k P_{k-1} V_{k-1} \cdots P_1 V_1 | 0_{\mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}}\rangle\|^2 \leq 1 - \delta$ for any Hilbert space $\mathcal{P}$ and any sequence of unitary operators $P_1, \ldots, P_{k-1} \in \mathbf{U}(\mathcal{M} \otimes \mathcal{P})$. Then, for any sequence $\rho_1, \ldots, \rho_k \in \mathbf{D}(\mathcal{V} \otimes \mathcal{M})$ such that $\rho_1 = |0_{\mathcal{V} \otimes \mathcal{M}}\rangle\langle 0_{\mathcal{V} \otimes \mathcal{M}}|$ and $\mathrm{tr}\Pi V_k \rho_k V_k^\dagger \geq 1 - \varepsilon$,*

$$\sum_{j=1}^{k-1} F(\mathrm{tr}_{\mathcal{M}} V_j \rho_j V_j^\dagger, \mathrm{tr}_{\mathcal{M}} \rho_{j+1}) \leq (k-1) - \frac{(\sqrt{1-\varepsilon} - \sqrt{1-\delta})^2}{2(k-1)}.$$

Proof. Let $\mathcal{P}$ be a sufficiently large Hilbert space so that we can take a purification $|\psi_j\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ of ρ_j for each $2 \leq j \leq k-1$, and let $|\psi_1\rangle = |0_{\mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}}\rangle$. Notice that $|\psi_1\rangle$ is a purification of ρ_1, and $V_j|\psi_j\rangle$ is a purification of $V_j \rho_j V_j^\dagger$, for each $1 \leq j \leq k-1$. Let $\Delta_j = 1 - F(\mathrm{tr}_{\mathcal{M}} V_j \rho_j V_j^\dagger, \mathrm{tr}_{\mathcal{M}} \rho_{j+1})$ for each $1 \leq j \leq k-1$. It follows from Lemma 1 that there exists a unitary transformation $P_j \in \mathbf{U}(\mathcal{M} \otimes \mathcal{P})$ such that $\||\psi_{j+1}\rangle - P_j V_j|\psi_j\rangle\| \leq \sqrt{2\Delta_j}$, for each $1 \leq j \leq k-1$. Hence we have

$$\|\Pi V_k|\psi_k\rangle - \Pi V_k P_{k-1} V_{k-1} \cdots P_1 V_1|\psi_1\rangle\|$$
$$\leq \|V_k|\psi_k\rangle - V_k P_{k-1} V_{k-1} \cdots P_1 V_1|\psi_1\rangle\|$$
$$= \||\psi_k\rangle - P_{k-1} V_{k-1} \cdots P_1 V_1|\psi_1\rangle\|$$
$$\leq \||\psi_k\rangle - P_{k-1} V_{k-1}|\psi_{k-1}\rangle\| + \sum_{j=1}^{k-2} \|P_{k-1} V_{k-1} \cdots P_{j+1} V_{j+1}|\psi_{j+1}\rangle - P_{k-1} V_{k-1} \cdots P_j V_j|\psi_j\rangle\|$$
$$= \sum_{j=1}^{k-1} \||\psi_{j+1}\rangle - P_j V_j|\psi_j\rangle\|$$
$$\leq \sum_{j=1}^{k-1} \sqrt{2\Delta_j}.$$

On the other hand,

$$\|\Pi V_k|\psi_k\rangle\| \leq \|\Pi V_k|\psi_k\rangle - \Pi V_k P_{k-1} V_{k-1} \cdots P_1 V_1|\psi_1\rangle\| + \|\Pi V_k P_{k-1} V_{k-1} \cdots P_1 V_1|\psi_1\rangle\|$$
$$\leq \sum_{j=1}^{k-1} \sqrt{2\Delta_j} + \sqrt{1-\delta}.$$

Notice that $\|\Pi V_k|\psi_k\rangle\| \geq \sqrt{1-\varepsilon}$, since $|\psi_k\rangle$ is a purification of ρ_k and $\mathrm{tr}\Pi V_k\rho_k V_k^\dagger \geq 1-\varepsilon$. Therefore,

$$\sum_{j=1}^{k-1} \sqrt{\Delta_j} \geq \frac{\sqrt{1-\varepsilon}-\sqrt{1-\delta}}{\sqrt{2}},$$

and thus,

$$\sum_{j=1}^{k-1} F(\mathrm{tr}_\mathcal{M} V_j\rho_j V_j^\dagger, \mathrm{tr}_\mathcal{M}\rho_{j+1}) = \sum_{j=1}^{k-1}(1-\Delta_j) = (k-1) - \sum_{j=1}^{k-1}\Delta_j \leq (k-1) - \frac{(\sqrt{1-\varepsilon}-\sqrt{1-\delta})^2}{2(k-1)},$$

as desired. $\qquad\square$

Using Lemma 16, we can show that our modified parallelization protocol above indeed works well, and we have the following lemma.

Lemma 17. *Let $m\colon \mathbb{Z}^+ \to \mathbb{N}$ be a polynomially bounded function and let $\varepsilon, \delta\colon \mathbb{Z}^+ \to [0,1]$ be any functions such that $m \geq 4$ and $\varepsilon < \frac{\delta^2}{16(m+1)^2}$. Then, $\mathrm{HVQPZK}(m, 1-\varepsilon, 1-\delta) \subseteq \mathrm{HVQPZK}\left(3, 1-\frac{\varepsilon}{2}, 1-\frac{\delta^2}{32(m+1)^2}\right)$.*

Proof. Let $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ be a problem in $\mathrm{HVQPZK}(m, 1-\varepsilon, 1-\delta)$ and let V be the corresponding m-message honest quantum verifier. For simplicity, it is assumed that m takes only even values (if $m(n)$ is odd for some $n \in \mathbb{Z}^+$, we modify the protocol so that the verifier sends a "dummy" message to a prover as the first message when the input has length n such that $m(n)$ is odd). Let V be the quantum register consisting of all the qubits in the private space of V, and let M be that consisting of all the qubits in the message channel between V and the prover. For every input x, V applies V_j for his jth transformation to the qubits in (V, M) for $1 \leq j \leq \frac{m}{2}+1$, and performs the measurement $\Pi = \{\Pi_{\mathrm{acc}}, \Pi_{\mathrm{rej}}\}$ at the end of the original protocol to decide acceptance or rejection. We construct a protocol of a three-message honest quantum verifier W.

For every input x, at the first message the new verifier W receives quantum registers V_j and M_j from the prover, for $2 \leq j \leq \frac{m}{2}+1$, where each V_j and M_j consist of the same number of qubits as V and M, respectively. W expects that the qubits in $(\mathsf{V}_j, \mathsf{M}_j)$ form the quantum state the original m-message verifier V would possess just after the $2(j-1)$-st message (i.e., just before the jth transformation of the verifier) of the original protocol, for $2 \leq j \leq \frac{m}{2}+1$.

Now W prepares quantum registers V_1 and M_1, which consist of the same number of qubits as V and M, respectively, and also prepares single-qubit quantum registers X and Y. W initializes all the qubits in V_1 and M_1 to state $|0\rangle$, while prepares $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ in (X, Y). W then chooses $r \in \left\{1, \ldots, \frac{m}{2}\right\}$ uniformly at random, applies V_r to the qubits in $(\mathsf{V}_r, \mathsf{M}_r)$, and sends Y and M_r together with r to the prover.

At the third message, W receives the quantum registers Y and M_r from the prover. Now W chooses $b \in \{0,1\}$ uniformly at random. If $b = 0$, W applies $V_{\frac{m}{2}+1}$ to the qubits in $(\mathsf{V}_{\frac{m}{2}+1}, \mathsf{M}_{\frac{m}{2}+1})$, and accepts if and only if the content of $(\mathsf{V}_{\frac{m}{2}+1}, \mathsf{M}_{\frac{m}{2}+1})$ corresponds to an accepting state in the original protocol. On the other hand, if $b = 1$, W first performs a controlled-swap between $(\mathsf{V}_r, \mathsf{M}_r)$ and $(\mathsf{V}_{r+1}, \mathsf{M}_{r+1})$ using the qubit in X as the control, then performs a controlled-not over the qubits in (X, Y) again using the qubit in X as the control, and finally applies the Hadamard transformation to the qubit in X. W accepts if and only if the qubit in X is in state $|0\rangle$.

The precise description of the protocol of W is found in Figure 1.

For the completeness, suppose that the input x is in A_{yes}.

Let P be the m-message honest quantum prover for the original proof system, and let P be the quantum register consisting of all the qubits in the private space of P. Denote by $\mathcal{V}$, $\mathcal{M}$, and $\mathcal{P}$ the Hilbert spaces corresponding to the registers V, M, and P, respectively. Let $|\psi_1\rangle = |0_{\mathcal{V}\otimes\mathcal{M}\otimes\mathcal{P}}\rangle$ be the quantum state in $(\mathsf{V}, \mathsf{M}, \mathsf{P})$, and let $|\psi_j\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ be the quantum state in $(\mathsf{V}, \mathsf{M}, \mathsf{P})$ just after the $2(j-1)$-st message (i.e., just before the jth transformation of the verifier) of the original protocol if V communicates with P on input x, for $2 \leq j \leq \frac{m}{2}+1$.

Honest Verifier's Three-Message Protocol

1. Receive quantum registers V_j and M_j from the prover, for $2 \leq j \leq \frac{m}{2} + 1$.

2. Prepare quantum registers V_1 and M_1 and single-qubit quantum registers X and Y. Initialize all the qubits in V_1 and M_1 to state $|0\rangle$, and prepare $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ in (X, Y). Choose $r \in \{1, \ldots, \frac{m}{2}\}$ uniformly at random and apply V_r to the qubits in (V_r, M_r). Send Y and M_r together with r to the prover.

3. Receive the quantum registers Y and M_r from the prover. Choose $b \in \{0, 1\}$ uniformly at random.

   3.1 If $b = 0$, do the following:
   Apply $V_{\frac{m}{2}+1}$ to the qubits in $(V_{\frac{m}{2}+1}, M_{\frac{m}{2}+1})$. Accept if the content of $(V_{\frac{m}{2}+1}, M_{\frac{m}{2}+1})$ corresponds to an accepting state in the original protocol, and reject otherwise.

   3.2 If $b = 1$, do the following:
   Perform a controlled-swap between (V_r, M_r) and (V_{r+1}, M_{r+1}) using the qubit in X as the control, and then perform a controlled-not over the qubits in (X, Y) again using the qubit in X as the control. Apply the Hadamard transformation to the qubit in X. Accept if the qubit in X is in state $|0\rangle$, and reject otherwise.

Figure 1: Honest verifier's three-message protocol.

Let R be the honest quantum prover in the constructed three-message system. In addition to the registers V_j and M_j, R prepares the quantum register P_j in his private space, for $1 \leq j \leq \frac{m}{2} + 1$, where each P_j consists of the same number of qubits as P. R prepares $|0_{\mathcal{P}}\rangle$ in P_1 so that the qubits in (V_1, M_1, P_1) form $|\psi_1\rangle$. At the first message of the constructed protocol, R generates $|\psi_j\rangle$ in (V_j, M_j, P_j), and sends V_j and M_j to W, for each $2 \leq j \leq \frac{m}{2} + 1$.

At the third message, if R receives r together with the registers Y and M_r, R applies P_r to the qubits in (M_r, P_r), where P_j is the jth transformation of the original prover P for each $1 \leq j \leq \frac{m}{2}$, and then performs a controlled-swap between P_r and P_{r+1} using the qubit in Y as the control. R then sends Y and M_r back to W.

It is obvious that R can convince W with probability at least $1 - \varepsilon$ if $b = 0$ is chosen by W at Step 3, since the qubits in $(V_{\frac{m}{2}+1}, M_{\frac{m}{2}+1})$ form the quantum state $\mathrm{tr}_{\mathcal{P}}|\psi_{\frac{m}{2}+1}\rangle\langle\psi_{\frac{m}{2}+1}|$. From the construction of R, it is also routine to show that R can convince W with certainty if $b = 1$ is chosen by W at Step 3, since $P_r V_r|\psi_r\rangle = |\psi_{r+1}\rangle$ for any r chosen from $\{1, \ldots, \frac{m}{2}\}$. Hence, W accepts every input $x \in A_{\mathrm{yes}}$ with probability at least $1 - \frac{\varepsilon}{2}$.

Next, for the soundness, suppose that the input x is in A_{no}.

Let R' be any three-message quantum prover for the constructed proof system. Let $\rho_j \in \mathbf{D}(\mathcal{V} \otimes \mathcal{M})$ be the reduced state in (V_j, M_j) of the entire system state just after the first transformation of R', for each $1 \leq j \leq \frac{m}{2} + 1$.

Consider the case in which W chooses r from $\{1, \ldots, \frac{m}{2}\}$ in Step 2 and also chooses $b = 1$ at Step 3. Then the probability that R' can convince W in this case cannot be larger than $\frac{1}{2} + \frac{1}{2}F(\mathrm{tr}_{\mathcal{M}}V_r\rho_r V_r^{\dagger}, \mathrm{tr}_{\mathcal{M}}\rho_{r+1})$ by an argument similar to that in the proof of Theorem 4 in Ref. [20]. Hence, the probability that R' can convince W when $b = 1$ is chosen at Step 3 is at most $\frac{1}{2} + \frac{1}{m}\sum_{j=1}^{\frac{m}{2}}F(\mathrm{tr}_{\mathcal{M}}V_j\rho_j V_j^{\dagger}, \mathrm{tr}_{\mathcal{M}}\rho_{j+1})$.

Now, if $\mathrm{tr}\Pi_{\mathrm{acc}}V_{\frac{m}{2}+1}\rho_{\frac{m}{2}+1}V_{\frac{m}{2}+1}^{\dagger} \geq 1 - \frac{\delta}{4}$, Lemma 16 implies that

$$\sum_{j=1}^{\frac{m}{2}} F(\mathrm{tr}_{\mathcal{M}}V_j\rho_j V_j^{\dagger}, \mathrm{tr}_{\mathcal{M}}\rho_{j+1})$$

$$\leq \frac{m}{2} - \frac{1}{m}\left(\sqrt{1 - \frac{\delta}{4}} - \sqrt{1 - \delta}\right)^2 \leq \frac{m}{2} - \frac{1}{m}\left[\left(1 - \frac{\delta}{4}\right) - \left(1 - \frac{\delta}{2}\right)\right]^2 = \frac{m}{2} - \frac{\delta^2}{16m},$$

12

and thus, the probability that R' can convince W when $b = 1$ is chosen is at most $\frac{1}{2} + \frac{1}{m}\left(\frac{m}{2} - \frac{\delta^2}{16m}\right) = 1 - \frac{\delta^2}{16m^2}$.

On the other hand, if $\mathrm{tr}\Pi_{\mathrm{acc}}V_{\frac{m}{2}+1}\rho_{\frac{m}{2}+1}V_{\frac{m}{2}+1}^\dagger \leq 1 - \frac{\delta}{4}$, it is obvious that R' can convince W with probability at most $1 - \frac{\delta}{4} \leq 1 - \frac{\delta^2}{16m^2}$ if $b = 0$ is chosen by W at Step 3, since the qubits in $\mathsf{V}_{\frac{m}{2}+1}$ and $\mathsf{M}_{\frac{m}{2}+1}$ are never touched by the prover after Step 1.

Hence the probability that R' can convince W for every input $x \in A_{\mathrm{no}}$ is at most $1 - \frac{\delta^2}{32m^2}$. Taking it into account that $m(n)$ may be odd for some $n \in \mathbb{Z}^+$, we have the bound of $1 - \frac{\delta^2}{32(m+1)^2}$.

Finally, the perfect zero-knowledge property against W is almost straightforward.

Let S_V be the simulator for the original m-message system such that, if x is in A_{yes}, the states $S_V(x, j)$ and $\mathrm{view}_{V,P}(x, j)$ are identical for each $1 \leq j \leq \frac{m}{2}$.

The simulator T_W for the constructed three-message system behaves as follows. For convenience, let R be the quantum register that is used to store the classical information r chosen by W, and let $S_V(x, 0) = |0_{\mathcal{V} \otimes \mathcal{M}}\rangle\langle 0_{\mathcal{V} \otimes \mathcal{M}}|$.

To simulate the state just after the first transformation of the prover R, T_W prepares the state $S_V(x, j - 1)$ in $(\mathsf{V}_j, \mathsf{M}_j)$, for each $2 \leq j \leq \frac{m}{2} + 1$, and outputs the state in $(\mathsf{V}_2, \mathsf{M}_2, \ldots, \mathsf{V}_{\frac{m}{2}+1}, \mathsf{M}_{\frac{m}{2}+1})$ as $T_W(x, 1)$.

To simulate the state just after the second transformation of the prover R, T_W first chooses $r \in \{1, \ldots, \frac{m}{2}\}$ uniformly at random, and sets the content of R to r. Next T_W prepares the state $S_V(x, j - 1)$ in $(\mathsf{V}_j, \mathsf{M}_j)$, for each $1 \leq j \leq r - 1$ and $r + 1 \leq j \leq \frac{m}{2} + 1$, and prepares the state $S_V(x, r)$ in $(\mathsf{V}_r, \mathsf{M}_r)$. T_W then prepares the state $|\Phi^+\rangle$ in (X, Y), and performs a controlled-swap between $(\mathsf{V}_r, \mathsf{M}_r)$ and $(\mathsf{V}_{r+1}, \mathsf{M}_{r+1})$ using the qubit in X as the control. Now T_W outputs the state in $(\mathsf{R}, \mathsf{X}, \mathsf{Y}, \mathsf{V}_1, \mathsf{M}_1, \ldots, \mathsf{V}_{\frac{m}{2}+1}, \mathsf{M}_{\frac{m}{2}+1})$ as $T_W(x, 2)$.

It is obvious that the ensemble $\{T_W(x, j)\}$ is polynomial-time preparable.

Suppose that x is in A_{yes}.

That $T_W(x, 1) = \mathrm{view}_{W,R}(x, 1)$ is obvious from the fact that $S_V(x, j) = \mathrm{view}_{V,P}(x, j)$ for $1 \leq j \leq \frac{m}{2}$.

To show that $T_W(x, 2) = \mathrm{view}_{W,R}(x, 2)$, let $\mathrm{view}_{V,P}(x, 0) = S_V(x, 0) = |0_{\mathcal{V} \otimes \mathcal{M}}\rangle\langle 0_{\mathcal{V} \otimes \mathcal{M}}|$, for convenience. Let σ_r and ξ_r be the quantum states in $(\mathsf{R}, \mathsf{X}, \mathsf{Y}, \mathsf{V}_1, \mathsf{M}_1, \ldots, \mathsf{V}_{\frac{m}{2}+1}, \mathsf{M}_{\frac{m}{2}+1})$ such that

$$\sigma_r = |r\rangle\langle r| \otimes |\Phi^+\rangle\langle\Phi^+| \otimes S_V(x, 0) \otimes \cdots \otimes S_V(x, r - 2) \otimes S_V(x, r) \otimes S_V(x, r) \otimes \cdots \otimes S_V\left(x, \frac{m}{2}\right)$$

and

$$\xi_r = |r\rangle\langle r| \otimes |\Phi^+\rangle\langle\Phi^+|$$
$$\otimes \mathrm{view}_{V,P}(x, 0) \otimes \cdots \otimes \mathrm{view}_{V,P}(x, r - 2) \otimes \mathrm{view}_{V,P}(x, r) \otimes \mathrm{view}_{V,P}(x, r) \otimes \cdots \otimes \mathrm{view}_{V,P}\left(x, \frac{m}{2}\right)$$

for each $1 \leq r \leq \frac{m}{2}$. Then, we have $\sigma_r = \xi_r$ for each $1 \leq r \leq \frac{m}{2}$, since $S_V(x, j) = \mathrm{view}_{V,P}(x, j)$ for $0 \leq j \leq \frac{m}{2}$. For each $1 \leq r \leq \frac{m}{2}$, let σ_r' and ξ_r' be the quantum states obtained by performing a controlled-swap between $(\mathsf{V}_r, \mathsf{M}_r)$ and $(\mathsf{V}_{r+1}, \mathsf{M}_{r+1})$ on σ_r and ξ_r, respectively, using the qubit in X as the control. Obviously, $\sigma_r' = \xi_r'$ for each $1 \leq r \leq \frac{m}{2}$. By definition, $T_W(x, 2) = \frac{2}{m}\sum_{r=1}^{\frac{m}{2}}\sigma_r'$. Furthermore, $\mathrm{view}_{W,R}(x, 2)$ is exactly the state $\frac{2}{m}\sum_{r=1}^{\frac{m}{2}}\xi_r'$. Now that $T_W(x, 2) = \mathrm{view}_{W,R}(x, 2)$ follows from the fact that $\sigma_r' = \xi_r'$ for each $1 \leq r \leq \frac{m}{2}$.

Hence the honest-verifier perfect zero-knowledge property against W follows. $\qquad\square$

Next we show that the parallel repetition theorem for three-message quantum interactive proofs may be extended to the case of three-message honest-verifier quantum perfect zero-knowledge proof systems.

Lemma 18. *Let $c, s\colon \mathbb{Z}^+ \to [0, 1]$ be any functions such that $c > s$. Then, for any polynomially bounded function $k\colon \mathbb{Z}^+ \to \mathbb{N}$, $\mathrm{HVQPZK}(3, c, s) \subseteq \mathrm{HVQPZK}(3, c^k, s^k)$. More strongly, let Π be any three-message honest-verifier quantum perfect zero-knowledge proof system for a problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ with completeness accepting probability at least $c(n)$ and soundness accepting probability at most $s(n)$ for every input of length n. Consider another proof system Π' such that, for every input of length n, Π' carries out $k(n)$ attempts of Π in parallel and accepts iff*

13

all the $k(n)$ attempts result in acceptance in Π. Then Π' is a three-message honest-verifier quantum perfect zero-knowledge proof system for A with completeness accepting probability at least $c(n)^{k(n)}$ and soundness accepting probability at most $s(n)^{k(n)}$ for every input of length n.

Proof. The completeness and soundness conditions follow from the proof of Theorem 6 in Ref. [20]. The honest-verifier perfect zero-knowledge property is trivial. Let V be the honest quantum verifier in the original three-message system Π and let S_V be the corresponding simulator such that, if x is in A_{yes}, the state $S_V(x, j)$ perfectly simulates V's view after the jth transformation of the honest quantum prover, for each $1 \leq j \leq 2$. Let W be the honest quantum verifier in the constructed three-message system Π'. For every x and for each $1 \leq j \leq 2$, the simulator T_W for Π' just outputs $T_W(x, j) = S_V(x, j)^{\otimes k(|x|)}$. Now the honest-verifier perfect zero-knowledge property is obvious. □

From Lemmas 17 and 18, it is immediate to show the following lemma.

Lemma 19. *For any polynomially bounded function $p\colon \mathbb{Z}^+ \to \mathbb{N}$, $\text{HVQPZK} \subseteq \text{HVQPZK}(3, 1 - 2^{-p}, 2^{-p})$.*

Proof. By sequential repetition, we can show that, for any polynomially bounded function $m\colon \mathbb{Z}^+ \to \mathbb{N}$, for any functions $c, s\colon \mathbb{Z}^+ \to [0, 1]$ that satisfy $c - s \geq \frac{1}{q}$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$, and for any polynomially bounded function $p\colon \mathbb{Z}^+ \to \mathbb{N}$, there exists a polynomially bounded function $m'\colon \mathbb{Z}^+ \to \mathbb{N}$ such that $\text{HVQPZK}(m, c, s) \subseteq \text{HVQPZK}(m', 1 - 2^{-p^2}, 2^{-p^2})$. Now Lemma 17 implies that $\text{HVQPZK}(m', 1 - 2^{-p^2}, 2^{-p^2}) \subseteq \text{HVQPZK}\left(3, 1 - 2^{-p^2-1}, 1 - \frac{(1 - 2^{-p^2})^2}{32(m'+1)^2}\right)$. Finally, by parallel repetition for sufficiently many times (say, for $32p(|x|)(m'(|x|) + 2)^2$ times), from Lemma 18, we have that $\text{HVQPZK}\left(3, 1 - 2^{-p^2-1}, 1 - \frac{(1 - 2^{-p^2})^2}{32(m'+1)^2}\right) \subseteq \text{HVQPZK}(3, 1 - 2^{-p}, 2^{-p})$, which completes the proof. □

3.2 Converting Honest-Verifier Quantum Perfect Zero-Knowledge Proofs to Public-Coin Systems

Next we show that any three-message honest-verifier quantum perfect zero-knowledge system can be modified to a three-message public-coin one in which the message from the verifier consists of only one classical bit. Marriott and Watrous [23] showed such a claim in the case of usual quantum interactive proofs. We show that their construction preserves the honest-verifier perfect zero-knowledge property.

Lemma 20. *Let $\varepsilon, \delta\colon \mathbb{Z}^+ \to [0, 1]$ be any functions that satisfy $\delta > 1 - (1 - \varepsilon)^2$. Then, any problem having a three-message honest-verifier quantum perfect zero-knowledge system with completeness accepting probability at least $1 - \varepsilon$ and soundness accepting probability at most $1 - \delta$ has a three-message public-coin honest-verifier quantum perfect zero-knowledge system with completeness accepting probability at least $1 - \frac{\varepsilon}{2}$ and soundness accepting probability at most $\frac{1}{2} + \frac{\sqrt{1 - \delta}}{2}$ in which the message from the verifier consists of only one classical bit.*

Proof. The proof is essentially same as that of Theorem 5.4 in Ref. [23] except for the zero-knowledge property.

Let $A = \{A_{\text{yes}}, A_{\text{no}}\}$ be a problem in $\text{HVQPZK}(3, 1 - \varepsilon, 1 - \delta)$ and let V be the corresponding three-message quantum verifier. Let V be the quantum register consisting of all the qubits in the private space of V, and let M be that consisting of all the qubits in the message channel between V and the prover. For every input x, V applies V_1 and V_2 on the qubits in (V, M) for his first and second transformations, respectively. We construct a protocol of a three-message public-coin quantum verifier W.

For every input x, at the first message the constructed verifier W receives the quantum register V from the prover. W expects that the prover prepares the quantum register M in his private space and the qubits in (V, M) form the quantum state the original verifier V would possess just after the second message (i.e., just after the first transformation of V) of the original protocol.

At the second message, W chooses $b \in \{0, 1\}$ uniformly at random and sends b to the prover.

14

Honest Verifier's Protocol in Three-Message Public-Coin System

1. Receive a quantum register V from the prover.

2. Choose $b \in \{0, 1\}$ uniformly at random. Send b to the prover.

3. Receive a quantum register M from the prover.

    3.1 If $b = 0$, apply V_2 to the qubits in (V, M). Accept if the content of (V, M) corresponds to an accepting state of the original protocol, and reject otherwise.

    3.2 If $b = 1$, apply $V_1^\dagger$ to the qubits in (V, M). Accept if all the qubits in V are in state $|0\rangle$, and reject otherwise.

Figure 2: Honest verifier's protocol in a three-message public-coin system.

If $b = 0$, the prover is requested to send M, so that the qubits in (V, M) form the quantum state the original verifier V would possess just after the third message (i.e., just after the second transformation of the prover) of the original protocol. Now W applies V_2 to the qubits in (V, M) and accepts if and only if the content of (V, M) corresponds to an accepting state of the original protocol.

On the other hand, if $b = 1$, the prover is requested to send M so that the qubits in (V, M) form the quantum state the original verifier V would possess just after the second message (i.e., just after the first transformation of V) of the original protocol. Now W applies $V_1^\dagger$ to the qubits in (V, M) and accepts if and only if all the qubits in V are in state $|0\rangle$.

The precise description of the protocol of W is found in Figure 2.

First suppose that the input x is in A_{yes}.

Let P be the three-message honest quantum prover for the original proof system, and let P be the quantum register consisting of all the qubits in the private space of P. Let $|\psi_2\rangle$ be the quantum state in (V, M, P) just after the second message (i.e., just after the first transformation of V) of the original protocol if V communicates with P on input x.

Let R be the honest prover in the constructed public-coin system. In addition to the registers V and M, R prepares the quantum register P in his private space. At the first message of the constructed protocol, R first generates $|\psi_2\rangle$ in (V, M, P) and then sends V to W.

At the third message of the constructed protocol, if $b = 0$, R first applies P_2 to the qubits in (M, P), and then sends M to W, where P_2 is the second transformation of the original prover P on input x in the original protocol, while if $b = 1$, R does nothing and just sends M to W.

It is obvious that R can convince W with probability at least $1 - \varepsilon$ if $b = 0$, and with certainty if $b = 1$. Hence, W accepts every input $x \in A_{\text{yes}}$ with probability at least $1 - \frac{\varepsilon}{2}$.

The soundness property for the case the input x is in A_{no} follows with exactly the same argument as in the proof of Theorem 5.4 in Ref. [23].

Finally, the perfect zero-knowledge property against W is almost straightforward.

Let S_V be the simulator for V in the original system such that, if x is in A_{yes}, the states $S_V(x, j)$ and $\text{view}_{V,P}(x, j)$ are identical for each $1 \le j \le 2$. Let $\mathcal{M}$ be the Hilbert space corresponding to the quantum register M. The simulator T_W for the constructed public-coin system behaves as follows. For convenience, let R be the single-qubit register that is used to store the classical information representing the outcome b of a public coin flipped by W.

Let $T_W(x,1)$ and $T_W(x,2)$ be quantum states in V and in $(\mathsf{R},\mathsf{V},\mathsf{M})$, respectively, defined by

$$T_W(x,1) = \mathrm{tr}_{\mathcal{M}} V_1 S_V(x,1) V_1^{\dagger},$$

$$T_W(x,2) = \frac{1}{2}\big[|0\rangle\langle 0| \otimes S_V(x,2) + |1\rangle\langle 1| \otimes \big(V_1 S_V(x,1) V_1^{\dagger}\big)\big].$$

It is obvious that the ensemble $\{T_W(x,j)\}$ is polynomial-time preparable.

Suppose that x is in A_{yes}. It is obvious that $T_W(x,1) = \mathrm{view}_{W,R}(x,1)$, since $T_W(x,1) = \mathrm{tr}_{\mathcal{M}} V_1 S_V(x,1) V_1^{\dagger}$, $\mathrm{view}(W,R)_1 = \mathrm{tr}_{\mathcal{M}} V_1 \mathrm{view}_{V,P}(x,1) V_1^{\dagger}$, and $S_V(x,1) = \mathrm{view}_{V,P}(x,1)$. The fact $T_W(x,2) = \mathrm{view}_{W,R}(x,2)$ follows from the properties $\mathrm{view}_{W,R}(x,2) = \frac{1}{2}\big[|0\rangle\langle 0| \otimes \mathrm{view}_{V,P}(x,2) + |1\rangle\langle 1| \otimes \big(V_1 \mathrm{view}_{V,P}(x,1) V_1^{\dagger}\big)\big]$, $S_V(x,1) = \mathrm{view}_{V,P}(x,1)$, and $S_V(x,2) = \mathrm{view}_{V,P}(x,2)$.

Hence the claim follows. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

3.3 HVQPZK = QPZK

First notice that the quantum rewinding technique due to Watrous [34] perfectly works well for any three-message public-coin honest-verifier quantum perfect zero-knowledge protocol in which the message from the verifier consists of only one classical bit. That is, we can show the following lemma.

Lemma 21. *Any three-message public-coin honest-verifier quantum perfect zero-knowledge system such that the message from the verifier consists of only one classical bit is perfect zero-knowledge against any polynomial-time quantum verifier.*

Proof. Let $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ be a problem having a three-message public-coin honest-verifier quantum perfect zero-knowledge system such that the message from the verifier consists of only one classical bit. Let V and P be the corresponding three-message public-coin honest quantum verifier and three-message honest quantum prover, respectively. Let M and N be the quantum registers consisting of all the qubits sent to V at the first message and of those at the third message, respectively, and let R and S be the single-qubit registers that are used to store the classical information representing the outcome b of a public coin flipped by V, where R is inside the private space of V and S is sent to P.

Let S_V be the simulator for V such that, if x is in A_{yes}, the states $S_V(x,1)$ and $\mathrm{view}_{V,P}(x,1)$ consisting of qubits in M are identical and the states $S_V(x,2)$ and $\mathrm{view}_{V,P}(x,2)$ consisting of qubits in $(\mathsf{M},\mathsf{N},\mathsf{R})$ are also identical.

Consider a generating circuit Q of the quantum state $S_V(x,2)$. Without loss of generality, it is assumed that Q acts over the qubits in $(\mathsf{M},\mathsf{N},\mathsf{R},\mathsf{A})$, where A is the quantum register consisting of q_A qubits for some polynomially bounded function $q_A \colon \mathbb{Z}^+ \to \mathbb{N}$.

For any polynomial-time quantum verifier W and any auxiliary quantum state ρ for W stored in the quantum register X inside the private space of W, we construct an efficiently implementable admissible mapping Φ that corresponds to a simulator T_W for W. Without loss of generality it is assumed that the message from W consists of a single *classical* bit, since the honest prover can easily enforce this constraint by measuring the message from the verifier before responding to it. Let W be the quantum register consisting of all the qubits in the private space of W except for those in X and M after having sent the second message. We consider the procedure described in Figure 3, which is the implementation of Φ.

Suppose that the input x is in A_{yes}.

Since the state $\mathrm{view}_{V,P}(x,2)$ can be written of the form $\mathrm{view}_{V,P}(x,2) = \frac{1}{2}(\sigma_0 \otimes |0\rangle\langle 0| + \sigma_1 \otimes |1\rangle\langle 1|)$ for some quantum states σ_0 and σ_1 in (M,N), the state $S_V(x,2)$ must also be of the form $S_V(x,2) = \frac{1}{2}(\sigma_0 \otimes |0\rangle\langle 0| + \sigma_1 \otimes |1\rangle\langle 1|)$ from the honest-verifier perfect zero-knowledge property. Therefore, the probability of obtaining $|0\rangle$ as the measurement result in Step 5 is exactly equal to $\frac{1}{2}$ regardless of the auxiliary quantum state ρ, because $\mathrm{tr}_{\mathcal{N}} \sigma_0 = \mathrm{tr}_{\mathcal{N}} \sigma_1$ holds from the honest-verifier perfect zero-knowledge property of the

---

Simulator for General Verifier W

1. Store the auxiliary quantum state ρ in the quantum register X. Prepare the quantum registers S, W, M, N, R, and A, and further prepare a single qubit quantum register F. Initialize all the qubits in F, S, W, M, N, R, and A in state $|0\rangle$.

2. Apply the generating circuit Q of the quantum state $S_V(x, 2)$ to the qubits in (M, N, R, A).

3. Apply W_1 to the qubits in (S, W, X, M), where W_1 is the first transformation of the simulated verifier W.

4. Compute the exclusive-or of the contents of R and S and write the result in F.

5. Measure the qubit in F in the $\{|0\rangle, |1\rangle\}$ basis. If this results in $|0\rangle$, output the qubits in (W, X, M, N, R), otherwise apply $W_1^\dagger$ to the qubits in (S, W, X, M) and then apply $Q^\dagger$ to the qubits in (M, N, R, A).

6. Apply the phase-flip if all the qubits in F, S, W, M, N, R, and A are in state $|0\rangle$, apply Q to the qubits in (M, N, R, A), and apply W_1 to the qubits in (S, W, X, M). Output the qubits in (W, X, M, N, R).

Figure 3: Simulator for a general verifier W.

protocol, where $\mathcal{N}$ is the Hilbert space corresponding to N (recall that when communicating with the honest verifier V, the qubits in M are never touched by V until the final transformation of V).

Let $\xi_i = \Pi_i W_1 (|0_{\mathcal{S} \otimes \mathcal{W}}\rangle \langle 0_{\mathcal{S} \otimes \mathcal{W}}| \otimes \rho \otimes \sigma_i \otimes |i\rangle \langle i|) W_1^\dagger \Pi_i$ be an unnormalized state in (S, W, X, M, N, R) for each $i \in \{0, 1\}$, where $\Pi_i = |i\rangle \langle i|$ is the projection operator over the qubit in S, and $\mathcal{S}$ and $\mathcal{W}$ are the Hilbert spaces corresponding to S and W, respectively. Then, conditioned on the measurement result being $|0\rangle$ in Step 5, the output is the state $\mathrm{tr}_{\mathcal{S}}(\xi_0 + \xi_1)$.

Noticing that $\mathrm{tr}_{\mathcal{S}} \frac{\xi_i}{\mathrm{tr}\xi_i}$ is exactly the state the verifier W would possess after the third message when the second message from W is i and that the probability of the second message from W being i is exactly equal to $\mathrm{tr}\xi_i$ for each $i \in \{0, 1\}$, $\mathrm{tr}_{\mathcal{S}}(\xi_0 + \xi_1) = \mathrm{tr}\xi_0 \cdot \mathrm{tr}_{\mathcal{S}} \frac{\xi_0}{\mathrm{tr}\xi_0} + \mathrm{tr}\xi_1 \cdot \mathrm{tr}_{\mathcal{S}} \frac{\xi_1}{\mathrm{tr}\xi_1}$ is exactly the state W would possess after the third message. Thus, the quantum rewinding technique due to Watrous [34] perfectly works well, which is implemented in Steps 5 and 6.

This ensures the perfect zero-knowledge property against W, which completes the proof. $\qquad\square$

From Lemma 21, it is immediate to show that $\mathrm{HVQPZK} = \mathrm{QPZK}$, i.e., honest-verifier quantum perfect zero-knowledge equals general quantum perfect zero-knowledge.

Theorem 22. $\mathrm{HVQPZK} = \mathrm{QPZK}$.

Proof. That $\mathrm{HVQPZK} \supseteq \mathrm{QPZK}$ is trivial and we show that $\mathrm{HVQPZK} \subseteq \mathrm{QPZK}$. Now Lemma 21 together with Lemmas 19 and 20 implies that $\mathrm{HVQPZK} \subseteq \mathrm{QPZK}\left(3, 1 - 2^{-p}, \frac{1}{2} + 2^{-\frac{p}{2}-1}\right)$ for any polynomially bounded function $p \colon \mathbb{Z}^+ \to \mathbb{N}$. Therefore, the fact that sequential repetition works well for the protocols of quantum zero-knowledge proofs establishes the statement. $\qquad\square$

From the proof of Theorem 22, the following property also follows.

Theorem 23. *Any problem in* QPZK *has a public-coin quantum perfect zero-knowledge proof system.*

4 Computational Zero-Knowledge Case

4.1 HVQZK = QZK

With essentially same arguments as in the perfect zero-knowledge case, we can show that honest-verifier quantum zero-knowledge equals general quantum zero-knowledge for the computational zero-knowledge case.

First, we show the following lemma, which is the computational zero-knowledge version of Lemma 17. The proof is exactly the same as the proof of Lemma 17 except for the zero-knowledge property and the honest-verifier computational zero-knowledge property can be proved by fairly straightforward hybrid arguments.

Lemma 24. *Let* $m\colon \mathbb{Z}^+ \to \mathbb{N}$ *be a polynomially bounded function and let* $\varepsilon, \delta\colon \mathbb{Z}^+ \to [0,1]$ *be any functions such that* $m \geq 4$ *and* $\varepsilon < \frac{\delta^2}{16(m+1)^2}$. *Then,* $\mathrm{HVQZK}(m, 1-\varepsilon, 1-\delta) \subseteq \mathrm{HVQZK}\left(3, 1-\frac{\varepsilon}{2}, 1-\frac{\delta^2}{32(m+1)^2}\right)$.

Alternatively, we may show the computational zero-knowledge version of Theorem 4 in Ref. [20].

Next we show that the parallel repetition theorem for three-message quantum interactive proofs may be extended to the case of three-message honest-verifier quantum computational zero-knowledge proof systems, which is the the computational zero-knowledge version of Lemma 18. Again the proof is exactly the same as the proof of Lemma 18 except for the zero-knowledge property and the honest-verifier computational zero-knowledge property can be proved by fairly straightforward hybrid arguments.

Lemma 25. *Let* $c, s\colon \mathbb{Z}^+ \to [0,1]$ *be any functions such that* $c > s$. *Then, for any polynomially bounded function* $k\colon \mathbb{Z}^+ \to \mathbb{N}$, $\mathrm{HVQZK}(3, c, s) \subseteq \mathrm{HVQZK}(3, c^k, s^k)$. *More strongly, let* Π *be any three-message honest-verifier quantum computational zero-knowledge proof system for a problem* $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ *with completeness accepting probability at least* $c(n)$ *and soundness accepting probability at most* $s(n)$ *for every input of length* n. *Consider another proof system* Π' *such that, for every input of length* n, Π' *carries out* $k(n)$ *attempts of* Π *in parallel and accepts iff all the* $k(n)$ *attempts result in acceptance in* Π. *Then* Π' *is a three-message honest-verifier quantum computational zero-knowledge proof system for* A *with completeness accepting probability at least* $c(n)^{k(n)}$ *and soundness accepting probability at most* $s(n)^{k(n)}$ *for every input of length* n.

Now Lemma 26 below follows from the essentially same argument as in the proof of Lemma 19, using Lemmas 24 and 25.

Lemma 26. *For any polynomially bounded function* $p\colon \mathbb{Z}^+ \to \mathbb{N}$, $\mathrm{HVQZK} \subseteq \mathrm{HVQZK}(3, 1-2^{-p}, 2^{-p})$.

We can also show the following lemma, which is the computational zero-knowledge version of Lemma 20.

Lemma 27. *Let* $\varepsilon, \delta\colon \mathbb{Z}^+ \to [0,1]$ *be any functions that satisfy* $\delta > 1 - (1-\varepsilon)^2$. *Then, any problem having a three-message honest-verifier quantum computational zero-knowledge system with completeness accepting probability at least* $1-\varepsilon$ *and soundness accepting probability at most* $1-\delta$ *has a three-message public-coin honest-verifier quantum computational zero-knowledge system with completeness accepting probability at least* $1-\frac{\varepsilon}{2}$ *and soundness accepting probability at most* $\frac{1}{2} + \frac{\sqrt{1-\delta}}{2}$ *in which the message from the verifier consists of only one classical bit.*

Proof. We use the same protocol construction as in the proof of Lemma 20 and we only show the zero-knowledge property. In what follows, we use the same notations as in the proof of Lemma 20.

Let S_V be the simulator for the original system such that, if x is in A_{yes}, the states $S_V(x, j)$ and $\mathrm{view}_{V,P}(x, j)$ are computationally indistinguishable for each $1 \leq j \leq 2$. Let $\mathcal{M}$ be the Hilbert space corresponding to the quantum register M. As in the proof of Lemma 20, the simulator T_W for the constructed public-coin system behaves as follows. For convenience, as in the proof of Lemma 20, let R be the single-qubit register that is used to store the classical information representing the outcome b of a public coin flipped by W.

Let $T_W(x,1)$ and $T_W(x,2)$ be quantum states in V and in $(\mathsf{R},\mathsf{V},\mathsf{M})$, respectively, defined by

$$T_W(x,1) = \mathrm{tr}_{\mathcal{M}} V_1 S_V(x,1) V_1^{\dagger},$$
$$T_W(x,2) = \frac{1}{2}\big[|0\rangle\langle 0| \otimes S_V(x,2) + |1\rangle\langle 1| \otimes \big(V_1 S_V(x,1) V_1^{\dagger}\big)\big].$$

It is obvious that the ensemble $\{T_W(x,j)\}$ is polynomial-time preparable.

Suppose that x is in A_{yes}. The computational indistinguishability between $T_W(x,1)$ and $\mathrm{view}_{W,R}(x,1)$ is obvious since $T_W(x,1) = \mathrm{tr}_{\mathcal{M}} V_1 S_V(x,1) V_1^{\dagger}$, $\mathrm{view}(W,R)_1 = \mathrm{tr}_{\mathcal{M}} V_1 \mathrm{view}_{V,P}(x,1) V_1^{\dagger}$, and $S_V(x,1)$ and $\mathrm{view}_{V,P}(x,1)$ are computational indistinguishable. The computational indistinguishability between $T_W(x,2)$ and $\mathrm{view}_{W,R}(x,2)$ follows from the properties $\mathrm{view}_{W,R}(x,2) = \frac{1}{2}\big[|0\rangle\langle 0| \otimes \mathrm{view}_{V,P}(x,2) + |1\rangle\langle 1| \otimes \big(V_1 \mathrm{view}_{V,P}(x,1) V_1^{\dagger}\big)\big]$, the computational indistinguishability between $S_V(x,1)$ and $\mathrm{view}_{V,P}(x,1)$, and that between $S_V(x,2)$ and $\mathrm{view}_{V,P}(x,2)$.

Now the lemma follows. $\qquad\qquad\square$

Now applying the quantum rewinding technique due to Watrous [34], we show the computational zero-knowledge version of Lemma 21, that any three-message public-coin honest-verifier quantum computational zero-knowledge system such that the message from the verifier consists of only one classical bit is computational zero-knowledge against any dishonest quantum verifier.

Lemma 28. *Any three-message public-coin honest-verifier quantum computational zero-knowledge system such that the message from the verifier consists of only one classical bit is computational zero-knowledge against any polynomial-time quantum verifier.*

Proof. We use the same construction of the simulator as in the proof of Lemma 21. In what follows, we use the same notations as in the proof of Lemma 21.

Let S_V be the simulator for V such that, if x is in A_{yes}, the states $S_V(x,1)$ and $\mathrm{view}_{V,P}(x,1)$ consisting of qubits in M are computationally indistinguishable and the states $S_V(x,2)$ and $\mathrm{view}_{V,P}(x,2)$ consisting of qubits in $(\mathsf{M},\mathsf{N},\mathsf{R})$ are also computationally indistinguishable, and consider the simulator construction in Figure 3 in the proof of Lemma 21.

Suppose that the input x is in A_{yes}.

We shall show that (i) the gap between $\frac{1}{2}$ and the probability of obtaining $|0\rangle$ as the measurement result in Step 5 must be negligible regardless of the auxiliary quantum state ρ, and (ii) the output state in Step 5 in the construction conditioned on the measurement result being $|0\rangle$ must be computationally indistinguishable from the state W would possess after the third message. With these two properties, the quantum rewinding technique due to Watrous [34] works well, by using the amplification lemma for the case with negligible perturbations, which is also due to Watrous [34]. This ensures the computational zero-knowledge property against W.

For the generating circuit Q' of the quantum state $\mathrm{view}_{V,P}(x,2)$ (for example, the unitary circuit P_1 that corresponds to the first transformation of the honest prover P realizes Q'), consider the "ideal" construction of the simulator such that Q' is applied instead of Q in Step 2 of the "real" simulator construction.

We first show the property (i).

Since the state $\mathrm{view}_{V,P}(x,2)$ can be written of the form $\mathrm{view}_{V,P}(x,2) = \frac{1}{2}(\sigma_0 \otimes |0\rangle\langle 0| + \sigma_1 \otimes |1\rangle\langle 1|)$ for some quantum states σ_0 and σ_1 in (M,N), the probability of obtaining $|0\rangle$ as the measurement result in Step 5 in the "ideal" construction is exactly equal to $\frac{1}{2}$ regardless of the auxiliary quantum state ρ, because $\mathrm{tr}_{\mathcal{N}}\sigma_0 = \mathrm{tr}_{\mathcal{N}}\sigma_1$ necessarily holds in this case, where $\mathcal{N}$ is the Hilbert space corresponding to N.

Now, from the honest-verifier computational zero-knowledge property, the states $S_V(x,2)$ and $\mathrm{view}_{V,P}(x,2)$ in $(\mathsf{M},\mathsf{N},\mathsf{R})$ are computationally indistinguishable. Since the circuit implementing W_1 is of size polynomial with respect to $|x|$, it follows that the gap between $\frac{1}{2}$ and the probability of obtaining $|0\rangle$ as the measurement result in Step 5 in the "real" construction must be negligible regardless of the auxiliary quantum state ρ, which proves the property (i).

Now we show the property (ii).

Let $\xi_i = \Pi_i W_1(|0_{\mathcal{S} \otimes \mathcal{W}}\rangle\langle 0_{\mathcal{S} \otimes \mathcal{W}}| \otimes \rho \otimes \sigma_i \otimes |i\rangle\langle i|) W_1^\dagger \Pi_i$ be an unnormalized state in $(\mathsf{S}, \mathsf{W}, \mathsf{X}, \mathsf{M}, \mathsf{N}, \mathsf{R})$ for each $i \in \{0, 1\}$, where $\Pi_i = |i\rangle\langle i|$ is the projection operator over the qubits in S, and $\mathcal{S}$ and $\mathcal{W}$ are the Hilbert spaces corresponding to S and W, respectively. Then, in the "ideal" construction, conditioned on the measurement result being $|0\rangle$ in Step 5, the output is the state $\mathrm{tr}_{\mathcal{S}}(\xi_0 + \xi_1)$.

Noticing that $\mathrm{tr}_{\mathcal{S}} \frac{\xi_i}{\mathrm{tr}\xi_i}$ is exactly the state the verifier W would possess after the third message when the second message from W is i and that the probability of the second message from W being i is exactly equal to $\mathrm{tr}\xi_i$ for each $i \in \{0, 1\}$, $\mathrm{tr}_{\mathcal{S}}(\xi_0 + \xi_1) = \mathrm{tr}\xi_0 \cdot \mathrm{tr}_{\mathcal{S}} \frac{\xi_0}{\mathrm{tr}\xi_0} + \mathrm{tr}\xi_1 \cdot \mathrm{tr}_{\mathcal{S}} \frac{\xi_1}{\mathrm{tr}\xi_1}$ is exactly the state W would possess after the third message.

Towards a contradiction, suppose that the output state in Step 5 in the "real" construction conditioned on the measurement result being $|0\rangle$ is computationally distinguishable from $\mathrm{tr}_{\mathcal{S}}(\xi_0 + \xi_1)$, which is the state W would possess after the third message. Let D be the corresponding distinguisher that uses the auxiliary quantum state ρ'. We construct a distinguisher D' for $S_V(x, 2)$ and $\mathrm{view}_{V,P}(x, 2)$ from D.

On input quantum state ξ that is either $S_V(x, 2)$ or $\mathrm{view}_{V,P}(x, 2)$, D' uses the auxiliary quantum state $\rho \otimes \rho'$, where ρ is the auxiliary quantum state the verifier W would use. D' prepares the quantum registers $\mathsf{S}, \mathsf{W}, \mathsf{M}, \mathsf{N}, \mathsf{R}$ and another quantum register Y. D' stores ρ in the register X, ξ in the register $(\mathsf{M}, \mathsf{N}, \mathsf{R})$, and ρ' in Y. All the qubits in S and W are initialized in state $|0\rangle$. Now D' applies W_1 to the qubits in $(\mathsf{S}, \mathsf{W}, \mathsf{X}, \mathsf{M})$, and then applies D to the qubits in $(\mathsf{W}, \mathsf{X}, \mathsf{M}, \mathsf{N}, \mathsf{R}, \mathsf{Y})$.

It is obvious from this construction that D' with the auxiliary quantum state $\rho \otimes \rho'$ forms a distinguisher for $S_V(x, 2)$ and $\mathrm{view}_{V,P}(x, 2)$ if D with the auxiliary quantum state ρ' forms a distinguisher for the output state in Step 5 in the "real" simulator construction conditioned on the measurement result being $|0\rangle$ and the state $\mathrm{tr}_{\mathcal{S}}(\xi_0 + \xi_1)$. This contradicts the computational indistinguishability between $S_V(x, 2)$ and $\mathrm{view}_{V,P}(x, 2)$, and thus the property (ii) follows. $\qquad\square$

From Lemmas 26, 27, and 28, it is easy to show that honest-verifier quantum computational zero-knowledge equals general quantum computational zero-knowledge. The proof is essentially same as the proof of Theorem 22, and thus, the property that public-coin quantum computational zero-knowledge equals general quantum computational zero-knowledge also follows.

Theorem 29. $\mathrm{HVQZK} = \mathrm{QZK}$.

Theorem 30. *Any problem in* QZK *has a public-coin quantum computational zero-knowledge proof system.*

4.2 QZK with Perfect Completeness Equals General QZK

In the computational zero-knowledge case, we can show that quantum computational zero-knowledge with one-sided bounded error of perfect completeness equals general quantum computational zero-knowledge.

The key idea is to show that any *honest-verifier* quantum computational zero-knowledge proof system with two-sided bounded error can be modified to that with one-sided bounded error of perfect completeness. This can be proved in a similar manner as in the proof of Theorem 2 of Ref. [20], but requires more careful analyses for showing the zero-knowledge property.

Lemma 31. *Let* $m \colon \mathbb{Z}^+ \to \mathbb{N}$ *be a polynomially bounded function, let* $\varepsilon \colon \mathbb{Z}^+ \to [0, 1]$ *be any negligible function such that there exists a polynomial-time uniformly generated family* $\{Q_{1^n}\}$ *of quantum circuits such that* Q_{1^n} *exactly performs the unitary transformation*

$$U_{\varepsilon(n)} = \begin{pmatrix} \sqrt{\varepsilon(n)} & \sqrt{1 - \varepsilon(n)} \\ \sqrt{1 - \varepsilon(n)} & -\sqrt{\varepsilon(n)} \end{pmatrix},$$

and let $\delta \colon \mathbb{Z}^+ \to [0, 1]$ *be any function that satisfies* $\delta > \varepsilon$. *Then,* $\mathrm{HVQZK}(m, 1 - \varepsilon, 1 - \delta) \subseteq \mathrm{HVQZK}(m + 2, 1, 1 - (\delta - \varepsilon)^2)$.

Honest Verifier's Protocol for Achieving Perfect Completeness

1. Prepare quantum registers V and M and a single-qubit quantum register X. Let Y be the single-qubit quantum register consisting of the qubit in V that corresponds to the output qubit of the original verifier. Initialize all the qubits in V, M, and X in state $|0\rangle$. Apply V_1 to the qubits in (V, M), and send M to the prover.

2. For $j = 2$ to $\frac{m}{2}$, do the following:
   Receive M from the prover. Apply V_j to the qubits in (V, M), and send M to the prover.

3. Receive B and M from the prover. Apply $V_{\frac{m}{2}+1}$ to the qubits in (V, M) and perform the Toffoli transformation over the qubits in $(\mathsf{X}, \mathsf{Y}, \mathsf{B})$ using the qubit in X as the target. Send V, M, and B to the prover.

4. Receive B from the prover. Perform a controlled-not over the qubits in (X, B) using the qubit in X as the control. Apply $U_\varepsilon^\dagger$ to the qubit in X. Accept if the content of X is 0, and reject otherwise.

Figure 4: Honest verifier's protocol for achieving perfect completeness

Proof. The proof is similar to the proof of Theorem 2 of Ref. [20], but requires more careful analyses for showing the zero-knowledge property.

Let $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ be a problem in $\mathrm{HVQZK}(m, 1 - \varepsilon, 1 - \delta)$, and let V be the corresponding m-message honest quantum verifier. Let V be the quantum register consisting of all the qubits in the private space of V, and let M be that consisting of all the qubits in the message channel between V and the prover. For every input x, V applies V_j for his jth transformation to the qubits in (V, M), for $1 \leq j \leq \lfloor \frac{m}{2} \rfloor + 1$. We construct a protocol of an $(m + 2)$-message honest quantum verifier W. For simplicity, in what follows, it is assumed that m is even (the cases in which m is odd can be proved in a similar manner).

For every input x, the new verifier W prepares the quantum registers V and M and another single-qubit quantum register X. Let Y be the single-qubit quantum register consisting of the qubit in V that corresponds to the output qubit of the original verifier V.

Using first $(m - 1)$ messages, W attempts to simulate the first $(m - 1)$ messages of the original m-message protocol, by applying V_j to the qubits in (V, M) as his jth transformation, for $1 \leq j \leq \frac{m}{2}$.

At the mth message, which is from the prover, W receives a single-qubit quantum register B in addition to M. W then applies $V_{\frac{m}{2}+1}$ to the qubits in (V, M), and further performs the Toffoli transformation over the qubits in $(\mathsf{B}, \mathsf{Y}, \mathsf{X})$, using the qubit in X as the target. Notice that the content of X is 1 if and only if the content of B is 1 and the state in (V, M) is an accepting state of the original protocol. Then W sends the registers B, V, and M to the prover, while keeping only X in his private.

At the last message of the protocol, W receives the qubit in B and verifies if the qubits in (X, B) form the state $|\phi\rangle = \sqrt{\varepsilon}|00\rangle + \sqrt{1 - \varepsilon}|11\rangle$.

The precise description of the protocol of W is described in Figure 4.

The soundness can be proved in almost the same way as in the proof of Theorem 2 of Ref. [20]. We show the completeness and the honest-verifier zero-knowledge properties. We first describe how the honest quantum prover behaves in the constructed $(m + 2)$-message system.

Suppose that the input x is in A_{yes}. Let P be the m-message honest quantum prover for the original proof system, and suppose that (V, P) accepts x with probability exactly $p_{\mathrm{acc}} \geq 1 - \varepsilon$. Let P be the quantum register consisting of all the qubits in the private space of P. Let P_j be the jth transformation of P on input x in the original protocol, for $1 \leq j \leq \frac{m}{2}$.

The $(m + 2)$-message honest quantum prover R for the constructed proof system prepares the register P and another single-qubit quantum register B in his private space. All the qubits in P and B are initially in state $|0\rangle$.

At the jth transformation of R, for $1 \leq j \leq \frac{m}{2} - 1$, after receiving the register M from W, R applies P_j to the qubits in (M, P) and sends M to W.

At the $\frac{m}{2}$th transformation of R, after receiving the register M from W, R first applies P_j to the qubits in (M, P). R also generates the state $|b\rangle = \sqrt{1 - \frac{1-\varepsilon}{p_{\mathrm{acc}}}}|0\rangle + \sqrt{\frac{1-\varepsilon}{p_{\mathrm{acc}}}}|1\rangle$ in the register B, and sends B and M to W.

Let $|\psi_{m+1}\rangle$ be the system state in (X, V, M, B) just after the $(m+1)$-st message of the constructed protocol, when W is communicating with R on the input x. Then $|\psi_{m+1}\rangle$ can be written as $|\psi_{m+1}\rangle = \alpha_0|0\rangle|\xi_0\rangle + \alpha_1|1\rangle|\xi_1\rangle$ for some states $|\xi_0\rangle$ and $|\xi_1\rangle$ in (V, M, B) orthogonal to each other, where $\alpha_1 = \sqrt{p_{\mathrm{acc}}} \cdot \sqrt{\frac{1-\varepsilon}{p_{\mathrm{acc}}}} = \sqrt{1-\varepsilon}$ and $\alpha_0 = \sqrt{1 - |\alpha_1|^2} = \sqrt{\varepsilon}$.

At the $\left(\frac{m}{2}+1\right)$-st transformation of R, after receiving the registers V, M, and B from W, R applies the unitary transformation Z to the qubits in (V, M, B) such that $Z|\xi_0\rangle = |\eta\rangle|0\rangle$ and $Z|\xi_1\rangle = |\eta\rangle|1\rangle$ for some state $|\eta\rangle$ in (V, M) (this is possible because $|\xi_0\rangle$ and $|\xi_1\rangle$ are orthogonal). R then sends B to W, which is the last message of the constructed protocol.

Now the perfect completeness is obvious from the constructions of W and R.

Finally, the zero-knowledge property against W is almost straightforward.

Let S_V be the simulator for the original m-message system such that, if x is in A_{yes}, the states $S_V(x, j)$ and $\mathrm{view}_{V,P}(x, j)$ are computationally indistinguishable, for each $1 \leq j \leq \frac{m}{2}$.

The simulator T_W for the constructed $(m+2)$-message system behaves as follows.

Let $T_W(x, j)$ be a quantum state in (X, V, M) defined by $T_W(x, j) = |0\rangle\langle 0| \otimes S_V(x, j)$ for each $1 \leq j \leq \frac{m}{2} - 1$. Let $T_W\left(x, \frac{m}{2}\right)$ be a quantum state in (X, V, M, B) defined by $T_W\left(x, \frac{m}{2}\right) = |0\rangle\langle 0| \otimes S_V\left(x, \frac{m}{2}\right) \otimes |1\rangle\langle 1|$. Finally, let $T_W\left(x, \frac{m}{2}+1\right)$ be a quantum state in (X, B) defined by $T_W\left(x, \frac{m}{2}+1\right) = |\phi\rangle\langle\phi|$. It is obvious that the ensemble $\{T_W(x, j)\}$ is polynomial-time preparable.

Suppose that x is in A_{yes}. For $1 \leq j \leq \frac{m}{2} - 1$, $T_W(x, j)$ is obviously computationally indistinguishable from $\mathrm{view}_{W,R}(x, j)$, since $T_W(x, j) = |0\rangle\langle 0| \otimes S_V(x, j)$, $\mathrm{view}_{W,R}(x, j) = |0\rangle\langle 0| \otimes \mathrm{view}_{V,P}(x, j)$, and $S_V(x, j)$ and $\mathrm{view}_{V,P}(x, j)$ are computationally indistinguishable. The computational indistinguishability between $T_W\left(x, \frac{m}{2}\right)$ and $\mathrm{view}_{W,R}\left(x, \frac{m}{2}\right)$ follows from the computational indistinguishability between $S_V\left(x, \frac{m}{2}\right)$ and $\mathrm{view}_{V,P}\left(x, \frac{m}{2}\right)$ and the fact that $\left\|\mathrm{view}_{W,R}\left(x, \frac{m}{2}\right) - |0\rangle\langle 0| \otimes \mathrm{view}_{V,P}\left(x, \frac{m}{2}\right) \otimes |1\rangle\langle 1|\right\|_{\mathrm{tr}} = \left\||b\rangle\langle b| - |1\rangle\langle 1|\right\|_{\mathrm{tr}} \leq 2\sqrt{1 - \frac{1-\varepsilon}{p_{\mathrm{acc}}}} \leq 2\sqrt{\varepsilon}$ is negligible. Finally, $T_W\left(x, \frac{m}{2}+1\right)$ and $\mathrm{view}_{W,R}\left(x, \frac{m}{2}+1\right)$ are identical, and thus, are trivially computationally indistinguishable. $\square$

Together with Lemmas 27 and 28 and the computational zero-knowledge version of Lemma 18, this implies the equivalence between quantum computational zero-knowledge with perfect completeness and usual quantum computational zero-knowledge with two-sided bounded error. The proof is similar to those of Theorems 22 and 29.

Theorem 32. *Any problem in* QZK *has a quantum computational zero-knowledge proof system of perfect completeness.*

Furthermore, in the computational zero-knowledge case, it is straightforward to extend Lemma 28 to the following more general statement.

Lemma 33. *Any three-message public-coin honest-verifier quantum computational zero-knowledge system such that the message from the verifier consists of $O(\log n)$ bits for every input of length n is computational zero-knowledge against any polynomial-time quantum verifier.*

Using Lemma 33, we can show the following.

Theorem 34. *Any problem in* QZK *has a three-message public-coin quantum computational zero-knowledge proof system of perfect completeness with soundness error probability at most $\frac{1}{p}$ for any polynomially bounded function $p: \mathbb{Z}^+ \to \mathbb{N}$ (hence with arbitrarily small constant error in soundness).*

Proof. Let $p\colon \mathbb{Z}^+ \to \mathbb{N}$ be any polynomially bounded function, and let $q\colon \mathbb{Z}^+ \to \mathbb{N}$ be a polynomially bounded function satisfying $2^{\frac{q}{2}} \geq \log p + 2$.

Then, from Lemmas 31 and 24 together with Lemma 25 for parallel repetition, we have that $\mathrm{HVQZK} \subseteq \mathrm{HVQZK}(3, 1, 2^{-q})$.

With Lemma 27, this further implies that any problem in HVQZK has a three-message public-coin honest-verifier quantum computational zero-knowledge proof system of perfect completeness with soundness accepting probability at most $\frac{1}{2} + 2^{-\frac{q}{2}-1}$ in which the message from the verifier consists of only one classical bit.

For every input of length n, we run this proof system $\lceil \log p(n) \rceil + 2$ times in parallel. From Lemma 25, this results in a three-message public-coin honest-verifier computational zero-knowledge proof system of perfect completeness with soundness accepting probability at most $\frac{1}{4p(n)}\big(1 + 2^{-\frac{q(n)}{2}}\big)^{\lceil \log p(n) \rceil + 2} \leq \frac{1}{p(n)}$ in which the message of the verifier consists of $\lceil \log p(n) \rceil + 2$ classical bits, for every input of length n.

Now Lemma 33 implies that this protocol is computational zero-knowledge even against any dishonest quantum verifier. Hence, any problem in QZK has a three-message public-coin quantum computational zero-knowledge proof system of perfect completeness with soundness error probability at most $\frac{1}{p}$, since $\mathrm{HVQZK} = \mathrm{QZK}$ by Theorem 29. □

5 Statistical Zero-Knowledge Case

All the properties shown for the computational zero-knowledge case also hold for the statistical zero-knowledge case. The proofs are essentially same as in the computational zero-knowledge case. This gives alternative proofs for the following theorems, which were originally shown by Watrous [34] using his previous results [32].

Theorem 35 ([32, 34])**.** $\mathrm{HVQSZK} = \mathrm{QSZK}$.

Theorem 36 ([32, 34])**.** *Any problem in* QSZK *has a public-coin quantum statistical zero-knowledge proof system.*

We also have the following new properties for quantum statistical zero-knowledge.

Theorem 37. *Any problem in* QSZK *has a quantum statistical zero-knowledge proof system of perfect completeness.*

Theorem 38. *Any problem in* QSZK *has a three-message public-coin quantum statistical zero-knowledge proof system of perfect completeness with soundness error probability at most $\frac{1}{p}$ for any polynomially bounded function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ (hence with arbitrarily small constant error in soundness).*

6 Equivalence of Two Definitions of Quantum Perfect Zero-Knowledge

In the classical case, the most common definition of perfect zero-knowledge proofs seems to allow the simulator to output "FAIL" with small probability, say, with probability at most $\frac{1}{2}$ [8, 28]. Following this convention, we may consider the following alternative definitions of honest-verifier and general quantum perfect zero-knowledge proof systems.

Definition 39. Given a polynomially bounded function $m\colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s\colon \mathbb{Z}^+ \to [0, 1]$, a problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ is in $\mathrm{HVQPZK}'(m, c, s)$ iff there exists an m-message honest quantum verifier V and an m-message honest quantum prover P such that

(Completeness and Soundness) (V, P) forms an m-message quantum interactive proof system with completeness accepting probability at least c and soundness accepting probability at most s,

(Honest-Verifier Perfect Zero-Knowledge) there exists a polynomial-time preparable ensembles $\{S_V(x,j)\}$ of quantum states such that, for every $x \in A_{\text{yes}}$ and for each $1 \le j \le \lceil \frac{m(|x|)}{2} \rceil$, $S_V(x,j) = p_{x,j}|0\rangle\langle 0| \otimes |0_{\mathcal{H}_j}\rangle\langle 0_{\mathcal{H}_j}| + (1 - p_{x,j})|1\rangle\langle 1| \otimes \text{view}_{V,P}(x,j)$ for some $0 \le p_{x,j} \le \frac{1}{2}$, where $\mathcal{H}_j$ is the Hilbert space $\text{view}_{V,P}(x,j)$ is in $\mathbf{D}(\mathcal{H}_j)$.

Definition 40. Given a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0,1]$, a problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in $\text{QPZK}'(m, c, s)$ iff there exists an m-message honest quantum verifier V and an m-message honest quantum prover P such that

(Completeness and Soundness) (V, P) forms an m-message quantum interactive proof system with completeness accepting probability at least c and soundness accepting probability at most s,

(Perfect Zero-Knowledge) for any m-message quantum verifier V', there exists a polynomial-time uniformly generated family $\{Q_x\}$ of quantum circuits, where each Q_x exactly implements an admissible transformation $S_{V'}(x)$, such that, for every $x \in A_{\text{yes}}$, $S_{V'}(x) = p_x(\Phi_0 \otimes \Psi_{\text{fail}}) + (1 - p_x)(\Phi_1 \otimes \langle V', P\rangle(x))$ for some $0 \le p_x \le \frac{1}{2}$, where $\langle V', P\rangle(x) \in \mathbf{T}(\mathcal{A}, \mathcal{Z})$ is the induced admissible transformation from V', P, and x for some Hilbert spaces $\mathcal{A}$ and $\mathcal{Z}$, $\Psi_{\text{fail}} \in \mathbf{T}(\mathcal{A}, \mathcal{Z})$ is the admissible transformation that always outputs $|0_{\mathcal{Z}}\rangle\langle 0_{\mathcal{Z}}|$, and Φ_b is the admissible transformation that takes nothing as input and outputs $|b\rangle\langle b|$, for each $b \in \{0, 1\}$.

In Definitions 39 and 40, the first qubit of the output of the simulator indicates whether or not the simulation succeeds — $|0\rangle\langle 0|$ is interpreted as failure and $|1\rangle\langle 1|$ as success.

Definition 41. A problem $A = \{A_{\text{yes}}, A_{\text{no}}\}$ is in HVQPZK' and in QPZK' if there exists a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ such that A is in $\text{HVQPZK}'\left(m, \frac{2}{3}, \frac{1}{3}\right)$ and in $\text{QPZK}'\left(m, \frac{2}{3}, \frac{1}{3}\right)$, respectively.

It is not obvious at a glance that $\text{HVQPZK} = \text{HVQPZK}'$ and $\text{QPZK} = \text{QPZK}'$, i.e., that the definitions of honest-verifier and general quantum perfect zero-knowledge proof systems using Definitions 4 and 10 is equivalent to those using Definitions 39 and 40.

Fortunately, using Theorem 22, we can show that $\text{HVQPZK} = \text{HVQPZK}'$ and $\text{QPZK} = \text{QPZK}'$. It is stressed that such equivalence is not known in the classical case.

Theorem 42. $\text{HVQPZK} = \text{HVQPZK}'$ *and* $\text{QPZK} = \text{QPZK}'$.

Proof. It is obvious that $\text{HVQPZK} \subseteq \text{HVQPZK}'$ and $\text{QPZK} \subseteq \text{QPZK}' \subseteq \text{HVQPZK}'$. From Theorem 22, we have $\text{HVQPZK} = \text{QPZK}$. Therefore, it is sufficient to show that $\text{HVQPZK}' \subseteq \text{HVQPZK}$.

Let $A = \{A_{\text{yes}}, A_{\text{no}}\}$ be a problem in $\text{HVQPZK}'\left(m, \frac{2}{3}, \frac{1}{3}\right)$ for some polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$. Without loss of generality, it is assumed that m takes only even values (if $m(n)$ is odd for some $n \in \mathbb{Z}^+$, we modify the protocol so that the verifier sends a "dummy" message to a prover as the first message when the input has length n such that $m(n)$ is odd). Let V and P be the corresponding honest verifier and honest prover, respectively. Let V be the quantum register consisting of all the qubits in the private space of V, and let M be that consisting of all the qubits in the message channel between V and the prover. For every input x, V applies V_j for his jth transformation to the qubits in (V, M) for $1 \le j \le \frac{m}{2} + 1$, and performs the measurement $\Pi = \{\Pi_{\text{acc}}, \Pi_{\text{rej}}\}$ at the end of the original protocol to decide acceptance or rejection. Let $\mathcal{V}$ and $\mathcal{M}$ be the Hilbert spaces corresponding to V and M, respectively.

Let $\{S_V(x, j)\}$ be the polynomial-time preparable ensembles of quantum states corresponding to the simulator for this honest-verifier quantum perfect zero-knowledge proof system such that, for every $x \in A_{\text{yes}}$ and for each $1 \le j \le \frac{m(|x|)}{2}$, $S_V(x, j) = p_{x,j}|0\rangle\langle 0| \otimes |0_{\mathcal{V} \otimes \mathcal{M}}\rangle\langle 0_{\mathcal{V} \otimes \mathcal{M}}| + (1 - p_{x,j})|1\rangle\langle 1| \otimes \text{view}_{V,P}(x, j)$ for some $0 \le p_{x,j} \le \frac{1}{2}$. This may be viewed as $S_V(x, j)$ outputting $|0\rangle\langle 0| \otimes |0_{\mathcal{V} \otimes \mathcal{M}}\rangle\langle 0_{\mathcal{V} \otimes \mathcal{M}}|$ with probability $p_{x,j}$

and $|1\rangle\langle 1| \otimes \text{view}_{V,P}(x,j)$ with probability $1 - p_{x,j}$. Without loss of generality, it is assumed that each $0 \le p_{x,j} \le 2^{-|x|}$, since we can easily amplify the success probability of the simulator by just running the original simulator a number of times so that a new simulator outputs $|0\rangle\langle 0| \otimes |0_{\mathcal{V}\otimes\mathcal{M}}\rangle\langle 0_{\mathcal{V}\otimes\mathcal{M}}|$ only if all the attempts result in $|0\rangle\langle 0| \otimes |0_{\mathcal{V}\otimes\mathcal{M}}\rangle\langle 0_{\mathcal{V}\otimes\mathcal{M}}|$.

First we slightly modify the behavior of the honest verifier as follows (call this modified honest verifier V'). At the beginning of the protocol, V' prepares a single-qubit quantum register B in addition to the registers V and M. The content of B will denote if the protocol successfully simulates the original protocol (that B contains 1 indicates the successful simulation). At the first transformation of V', V' prepares $|1\rangle$ in B and $V_1|0_{\mathcal{V}\otimes\mathcal{M}}\rangle$ in (V, M), and sends B and M to a prover. At every message from the prover, V' receives B in addition to the qubits in M the original verifier V would receive. At the jth transformation of V', V' applies V_j to the qubits in (V, M), for $2 \le j \le \frac{m(|x|)}{2} + 1$. That is, the jth transformation of V' is given by $V'_j = I \otimes V_j$, for $2 \le j \le \frac{m(|x|)}{2} + 1$. Then V' sends B and M back to the prover as the $(2j-1)$-st message, for $2 \le j \le \frac{m(|x|)}{2}$. At the end of the protocol, V' accepts if and only if the content of B is 1 and the content of (V, M) corresponds to an accepting state of the original protocol.

It is obvious that the soundness accepting probability is at most $\frac{1}{3}$, since it cannot be larger than that in the original protocol from the construction of V'.

To show the completeness and honest-verifier perfect zero-knowledge conditions, we construct a new honest prover P' as follows. Let P be the quantum register consisting of all the qubits in the private space of the original honest prover P. The new prover P' prepares P as well as single-qubit quantum registers B'_j and quantum registers V'_j and M'_j in his private space for $1 \le j \le \frac{m(|x|)}{2}$, where V'_j and M'_j consists of the same number of qubits as V and M, respectively. All the qubits in the registers P, B'_j, V'_j, and M'_j, for $1 \le j \le \frac{m(|x|)}{2}$, are initialized to state $|0\rangle$.

At the jth transformation of P', for $1 \le j \le \frac{m(|x|)}{2}$, after having received B and M, P' first measures the qubit in B in the $\{|0\rangle, |1\rangle\}$ basis to obtain the measurement outcome b.

If $b = 0$, P' does nothing and just sends B and M back to the verifier.

On the other hand, if $b = 1$, P' first generates $S_V(x,j)$ in $(\mathsf{B}'_j, \mathsf{V}'_j, \mathsf{M}'_j)$. If this results in $|0\rangle\langle 0| \otimes |0_{\mathcal{V}\otimes\mathcal{M}}\rangle\langle 0_{\mathcal{V}\otimes\mathcal{M}}|$, P' flips the content of B so that B now contains 0, and sends B and M back to the verifier. Otherwise P' applies P_j, the jth transformation of the original honest prover P, to the qubits in (M, P), and sends B and M back to the verifier (note that B always contains 1 in this case).

From the construction of P', it is easy to see that, if the input x is in A_{yes}, P' is accepted with probability at least $\frac{2}{3}(1 - 2^{-|x|})^{\frac{m(|x|)}{2}} \ge \frac{5}{9}$.

Next we construct a new simulator $S'_{V'}$ as follows. $S'_{V'}$ prepares the quantum registers B, V, and M and another three quantum registers B', V', and M', where B', V', and M' consists of the same number of qubits as B, V, and M, respectively. For convenience, let $S'_{V'}(x,0) = |1\rangle\langle 1| \otimes |0_{\mathcal{V}\otimes\mathcal{M}}\rangle\langle 0_{\mathcal{V}\otimes\mathcal{M}}|$. We define $S'_{V'}$ inductively with respect to j, for $1 \le j \le \frac{m(|x|)}{2}$.

Assume that the state $S'_{V'}(x, j-1)$ has already been defined. To simulate the state after the jth transformation of P', $S'_{V'}$ first generates $\rho_j = V'_j S'_{V'}(x, j-1) V'^\dagger_j$ in (B, V, M). If the content of B is 0, $S'_{V'}$ just outputs the state in (B, V, M). Otherwise if the content of B is 1, $S'_{V'}$ generates the state $S_V(x, j)$ in (B', V', M'). If the content of B' is 0, $S'_{V'}$ outputs the state in (B', V, M), otherwise if the content of B' is 1, $S'_{V'}$ outputs the state in (B', V', M').

Let Π_b be the projection defined by $\Pi_b = |b\rangle\langle b| \otimes I_{\mathcal{V}\otimes\mathcal{M}}$, for each $b \in \{0,1\}$. Then, $S'_{V'}(x,j)$ can be written as

$$S'_{V'}(x,j) = \Pi_0 \rho_j \Pi_0 + (\text{tr}\Pi_0 S_V(x,j))|0\rangle\langle 0| \otimes \text{tr}_{\mathcal{B}}\Pi_1 \rho_j \Pi_1 + (\text{tr}\Pi_1 \rho_j)\Pi_1 S_V(x,j)\Pi_1$$
$$= \Pi_0 \rho_j \Pi_0 + p_{x,j}|0\rangle\langle 0| \otimes \text{tr}_{\mathcal{B}}\Pi_1 \rho_j \Pi_1 + (\text{tr}\Pi_1 \rho_j)(1 - p_{x,j})|1\rangle\langle 1| \otimes \text{view}_{V,P}(x,j),$$

for $1 \le j \le \frac{m(|x|)}{2}$, where $\mathcal{B}$ is the Hilbert space corresponding to B.

It is easy to see that the ensemble $\{S'_{V'}(x,j)\}$ is polynomial-time preparable.

Suppose that x is in A_{yes}. We show by induction that $S'_{V'}(x, j) = \text{view}_{V', P'}(x, j)$ for each $1 \le j \le \frac{m(|x|)}{2}$. For convenience, let $\text{view}_{V', P'}(x, 0) = S'_{V'}(x, 0) = |1\rangle\langle 1| \otimes |0_{\mathcal{V} \otimes \mathcal{M}}\rangle\langle 0_{\mathcal{V} \otimes \mathcal{M}}|$, and let $\sigma_j = V'_j \text{view}_{V', P'}(x, j-1) V'^{\dagger}_j$ for each $1 \le j \le \frac{m(|x|)}{2}$.

In the case $j = 1$, it is obvious that $S'_{V'}(x, 1) = \text{view}_{V', P'}(x, 1)$, since

$$\rho_1 = \sigma_1 = V'_1(|1\rangle\langle 1| \otimes |0_{\mathcal{V} \otimes \mathcal{M}}\rangle\langle 0_{\mathcal{V} \otimes \mathcal{M}}|)V'^{\dagger}_1 = |1\rangle\langle 1| \otimes (V_1|0_{\mathcal{V} \otimes \mathcal{M}}\rangle\langle 0_{\mathcal{V} \otimes \mathcal{M}}|V^{\dagger}_1),$$

and thus

$$\begin{aligned}
S'_{V'}(x, 1) &= p_{x,1}|0\rangle\langle 0| \otimes \text{tr}_{\mathcal{B}}\Pi_1\rho_1\Pi_1 + (1 - p_{x,1})|1\rangle\langle 1| \otimes \text{view}_{V,P}(x, 1) \\
&= p_{x,1}|0\rangle\langle 0| \otimes \text{tr}_{\mathcal{B}}\Pi_1\sigma_1\Pi_1 + (1 - p_{x,1})|1\rangle\langle 1| \otimes \text{view}_{V,P}(x, 1) \\
&= \text{view}_{V', P'}(x, 1).
\end{aligned}$$

Suppose that $S'_{V'}(x, j) = \text{view}_{V', P'}(x, j)$ holds for all $1 \le j \le k$. We show the case $j = k + 1$. By definition,

$$S'_{V'}(x, k+1) = \Pi_0\rho_{k+1}\Pi_0 + (\text{tr}\Pi_0 S_V(x, k+1))|0\rangle\langle 0| \otimes \text{tr}_{\mathcal{B}}\Pi_1\rho_{k+1}\Pi_1 + (\text{tr}\Pi_1\rho_{k+1})\Pi_1 S_V(x, k+1)\Pi_1,$$

and notice that

$$\begin{aligned}
\text{view}_{V', P'}(x, k+1) = {}&\Pi_0\sigma_{k+1}\Pi_0 + (\text{tr}\Pi_0 S_V(x, k+1))|0\rangle\langle 0| \otimes \text{tr}_{\mathcal{B}}\Pi_1\sigma_{k+1}\Pi_1 \\
&+ (\text{tr}\Pi_1\sigma_{k+1})(\text{tr}\Pi_1 S_V(x, k+1))|1\rangle\langle 1| \otimes \text{view}_{V,P}(x, k+1).
\end{aligned}$$

Since $\rho_{k+1} = V'_{k+1} S'_{V'}(x, k) V'^{\dagger}_{k+1}$ and $\sigma_{k+1} = V'_{k+1}\text{view}_{V', P'}(x, k)V'^{\dagger}_{k+1}$, we have $\rho_{k+1} = \sigma_{k+1}$ from the assumption that $S'_{V'}(x, k) = \text{view}_{V', P'}(x, k)$. Furthermore, we have

$$\Pi_1 S_V(x, k+1)\Pi_1 = (\text{tr}\Pi_1 S_V(x, k+1))|1\rangle\langle 1| \otimes \text{view}_{V,P}(x, k+1).$$

Therefore, that $S'_{V'}(x, k+1) = \text{view}_{V', P'}(x, k+1)$ follows.

Hence, the honest-verifier perfect zero-knowledge property against P' holds in the sense of Definition 4.

Finally, recall that the success probability can be amplified using sequential repetition, and thus, that $\text{HVQPZK}' \subseteq \text{HVQPZK}$ follows. $\qquad\square$

7 Conclusion

This paper has established a unified framework that directly proves a number of general properties of quantum zero-knowledge proofs. Our method works well for any of quantum perfect, statistical, and computational zero-knowledge cases. We conclude by mentioning several open problems concerning quantum zero-knowledge proofs:

- We have proved that quantum computational and statistical zero-knowledge proofs can be made perfect complete. Can quantum *perfect* zero-knowledge proofs be made perfect complete?

- Although we have proved properties of quantum zero-knowledge proofs directly, natural complete problems or characterizations are definitely helpful when proving properties of quantum zero-knowledge proofs. Are their any natural complete problems or characterizations for QZK and QPZK?

- We have investigated the properties of QZK that hold unconditionally. On the other hand, Watrous [34] proved that every problem in NP has a quantum computational zero-knowledge proof system under some intractability assumptions. In the classical case, it is known that every problem in IP = PSPACE is provable in computational zero-knowledge under some intractability assumptions [18, 4, 22, 29]. How powerful are quantum computational zero-knowledge proofs under reasonable intractability assumptions?

Acknowledgement

The author would like to thank John Watrous for his helpful comments on the choice of the universal gate set.

References

[1] Dorit Aharonov, Alexei Yu. Kitaev, and Noam Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998.

[2] William Aiello and Johan Håstad. Statistical zero-knowledge languages can be recognized in two rounds. *Journal of Computer and System Sciences*, 42(3):327–345, 1991.

[3] Avraham Ben-Aroya and Amnon Ta-Shma. Quantum expanders and the quantum entropy difference problem. arXiv.org e-Print archive, quant-ph/0702129, 2007.

[4] Michael Ben-Or, Oded Goldreich, Shafi Goldwasser, Johan Håstad, Joe Kilian, Silvio Micali, and Phillip Rogaway. Everything provable is provable in zero-knowledge. In *Advances in Cryptology – CRYPTO '88, 8th Annual International Cryptology Conference*, volume 403 of *Lecture Notes in Computer Science*, pages 37–56, 1988.

[5] Ivan Dåmgard, Serge Fehr, and Louis Salvail. Zero-knowledge proofs and string commitments withstanding quantum attacks. In *Advances in Cryptology – CRYPTO 2004, 24th Annual International Cryptology Conference*, volume 3152 of *Lecture Notes in Computer Science*, pages 254–272, 2004.

[6] Shimon Even, Alan L. Selman, and Yacov Yacobi. The complexity of promise problems with applications to public-key cryptography. *Information and Control*, 61(2):159–173, 1984.

[7] Lance J. Fortnow. The complexity of perfect zero-knowledge. In Silvio Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 327–343. JAI Press, 1989.

[8] Oded Goldreich. *Foundations of Cryptography – Basic Tools*. Cambridge, 2001.

[9] Oded Goldreich. Zero-knowledge twenty years after its invention. Electronic Colloquium on Computational Complexity, Report No. 63, 2002.

[10] Oded Goldreich and Shafi Goldwasser. On the limits of nonapproximability of lattice problems. *Journal of Computer and System Sciences*, 60(3):540–463, 2000.

[11] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(3):691–729, 1991.

[12] Oded Goldreich, Amit Sahai, and Salil P. Vadhan. Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 399–408, 1998.

[13] Oded Goldreich, Amit Sahai, and Salil P. Vadhan. Can statistical zero knowledge be made non-interactive? or on the relationship of SZK and NISZK. In *Advances in Cryptology – CRYPTO '99, 19th Annual International Cryptology Conference*, volume 1666 of *Lecture Notes in Computer Science*, pages 467–484, 1999.

[14] Oded Goldreich and Salil P. Vadhan. Comparing entropies in statistical zero knowledge with applications to the structure of SZK. In *Fourteenth Annual IEEE Conference on Computational Complexity*, pages 54–73, 1999.

[15] Shafi Goldwasser, Silvio Micali, and Charles W. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[16] Jeroen van de Graaf. *Towards a formal definition of security for quantum protocols*. PhD thesis, Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, December 1997.

[17] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[18] Russell Impagliazzo and Moti Yung. Direct minimum-knowledge computations. In *Advances in Cryptology – CRYPTO '87, A Conference on the Theory and Applications of Cryptographic Techniques*, volume 293 of *Lecture Notes in Computer Science*, pages 40–51, 1988.

[19] Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[20] Alexei Yu. Kitaev and John H. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 608–617, 2000.

[21] Hirotada Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. In *Algorithms and Computation, 14th International Symposium, ISAAC 2003*, volume 2906 of *Lecture Notes in Computer Science*, pages 178–188, 2003.

[22] Carsten Lund, Lance J. Fortnow, Howard J. Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992.

[23] Chris Marriott and John H. Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[24] Moni Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4(2):151–158, 1991.

[25] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[26] Tatsuaki Okamoto. On relationships between statistical zero-knowledge proofs. *Journal of Computer and System Sciences*, 60(1):47–108, 2000.

[27] Bill Rosgen and John H. Watrous. On the hardness of distinguishing mixed-state quantum computations. In *Twentieth Annual IEEE Conference on Computational Complexity*, pages 344–354, 2005.

[28] Amit Sahai and Salil P. Vadhan. A complete problem for statistical zero knowledge. *Journal of the ACM*, 50(2):196–249, 2003.

[29] Adi Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992.

[30] Peter W. Shor. Fault-tolerant quantum computation. In *37th Annual Symposium on Foundations of Computer Science*, pages 56–65, 1996.

[31] Salil P. Vadhan. An unconditional study of computational zero-knowledge. *SIAM Journal on Computing*, 36(4):1160–1214, 2006.

[32] John H. Watrous. Limits on the power of quantum statistical zero-knowledge. In *43rd Annual Symposium on Foundations of Computer Science*, pages 459–468, 2002.

[33] John H. Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003.

[34] John H. Watrous. Zero-knowledge against quantum attacks. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, pages 296–305, 2006.

[35] John H. Watrous. Private communication. April, 2007.

Appendix

A Quantum Interactive Proof Systems

Here we review the model of quantum interactive proof systems. Although the term "round" is commonly used in classical interactive proofs for describing each set of verifier's question and corresponding prover's response, this paper follows the custom in the preceding papers of quantum interactive proofs [33, 20, 32, 23, 27] and uses the term "message" instead of "round". One round consists of two messages: the message from a verifier and the message from a prover.

A quantum interactive proof system consists of two parties: a quantum verifier V and a quantum prover P. Associated with the quantum interactive proof system are the Hilbert spaces $\mathcal{V}$, $\mathcal{M}$, and $\mathcal{P}$, where $\mathcal{V}$ corresponds to the private space of the verifier V, $\mathcal{M}$ corresponds to the space used for communication between the verifier V and the prover P, and $\mathcal{P}$ corresponds to the private space of the prover P.

For every input of length n, each space $\mathcal{V}$, $\mathcal{M}$, and $\mathcal{P}$ consists of $q_{\mathcal{V}}(n)$, $q_{\mathcal{M}}(n)$, and $q_{\mathcal{P}}(n)$ qubits, respectively, for some polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and some function $q_{\mathcal{P}} \colon \mathbb{Z}^+ \to \mathbb{N}$. Accordingly, the entire system consists of $q(n) = q_{\mathcal{V}}(n) + q_{\mathcal{M}}(n) + q_{\mathcal{P}}(n)$ qubits. Such a system is called $(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-*space-bounded*, and the associated verifier and prover are called $(q_{\mathcal{V}}, q_{\mathcal{M}})$-*space-bounded* and $(q_{\mathcal{M}}, q_{\mathcal{P}})$-*space-bounded*, respectively. One of the private qubits of the verifier is designated as the output qubit.

Formally, an m-*message* $(q_{\mathcal{V}}, q_{\mathcal{M}})$-space-bounded quantum verifier V for quantum interactive proof systems is a polynomial-time computable mapping of the form $V \colon \{0,1\}^* \to \{0,1\}^*$. For every n and for every input $x \in \{0,1\}^*$ of length n, V uses at most $q_{\mathcal{V}}(n)$ qubits for his private space and at most $q_{\mathcal{M}}(n)$ qubits for each communication with a prover. The string $V(x)$ is interpreted as a $\lceil (m(n)+1)/2 \rceil$-tuple $(V(x)_1, \ldots, V(x)_{\lceil (m(n)+1)/2 \rceil})$, with each $V(x)_j$ a description of a polynomial-time uniformly generated quantum circuit acting on $q_{\mathcal{V}}(n) + q_{\mathcal{M}}(n)$ qubits.

Similarly, an m-*message* $(q_{\mathcal{M}}, q_{\mathcal{P}})$-space-bounded quantum verifier P is a mapping of the form $P \colon \{0,1\}^* \to \{0,1\}^*$. For every n and for every input $x \in \{0,1\}^*$ of length n, P uses at most $q_{\mathcal{P}}(n)$ qubits for his private space and at most $q_{\mathcal{M}}(n)$ qubits for each communication with a verifier. The string $P(x)$ is interpreted as a $\lceil m(n)/2 \rceil$-tuple $(P(x)_1, \ldots, P(x)_{\lceil m(n)/2 \rceil})$, with each $P(x)_j$ a description of a quantum circuit acting on $q_{\mathcal{M}}(n) + q_{\mathcal{P}}(n)$ qubits. No restrictions are placed on the complexity of the mapping P (i.e., each $P(x)_j$ can be an arbitrary unitary transformation).

Given an m-message $(q_{\mathcal{V}}, q_{\mathcal{M}})$-space-bounded quantum verifier V, an m-message $(q_{\mathcal{M}}, q_{\mathcal{P}})$-space-bounded quantum prover P, and an input x of length n, we define a circuit $(V(x), P(x))$ acting over $\mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ of $q(n)$ qubits as follows. If $m(n)$ is odd, circuits $P(x)_1, V(x)_1, \ldots, P(x)_{(m(n)+1)/2}, V(x)_{(m(n)+1)/2}$ are applied in sequence, each $V(x)_j$ to $\mathcal{V} \otimes \mathcal{M}$ and each $P(x)_j$ to $\mathcal{M} \otimes \mathcal{P}$. If $m(n)$ is even, circuits $V(x)_1, P(x)_1, \ldots, V(x)_{m(n)/2}, P(x)_{m(n)/2}, V(x)_{m(n)/2+1}$ are applied in sequence.

At any given instant, the state of the entire system is a unit vector in the space $\mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$. At the beginning of the protocol, the system is in the initial state such that all the qubits in $\mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ are in state $|0\rangle$. In case V and/or P have some auxiliary quantum states ρ and/or σ at the beginning of protocol, the qubits in the private space of V and/or P corresponding to these auxiliary quantum states are initialized to ρ and/or σ, respectively. In such

a case, the state of the entire system may be in a mixed state in $\mathbf{D}(\mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P})$, and the descriptions below are interpreted in the context of mixed states with proper modifications.

For every input x of length n, the probability $p_{\mathrm{acc}}(x, V, P)$ that (V, P) accepts x is defined to be the probability that an observation of the output qubit in the $\{|0\rangle, |1\rangle\}$ basis yields $|1\rangle$, after the circuit $(V(x), P(x))$ is applied to the initial state $|\psi_{\mathrm{init}}\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$. Let Π_{acc} be the projection onto the space consisting of states whose output qubit is in state $|1\rangle$. Then, $p_{\mathrm{acc}}(x, V, P) = \|\Pi_{\mathrm{acc}} V(x)_{(m(n)+1)/2} P(x)_{(m(n)+1)/2} \cdots V(x)_1 P(x)_1 |\psi_{\mathrm{init}}\rangle\|^2$ if $m(n)$ is odd, and $p_{\mathrm{acc}}(x, V, P) = \|\Pi_{\mathrm{acc}} V(x)_{m(n)/2+1} P(x)_{m(n)/2} V(x)_{m(n)/2} \cdots P(x)_1 V(x)_1 |\psi_{\mathrm{init}}\rangle\|^2$ if $m(n)$ is even.

The class of problems having an m-message quantum interactive proof system with completeness accepting probability at least c and soundness accepting probability at most s is denoted by $\mathrm{QIP}(m, c, s)$. The following is the formal definition of the class $\mathrm{QIP}(m, c, s)$.

Definition 43. Given a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0, 1]$, a problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ is in $\mathrm{QIP}(m, c, s)$ iff there exist polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and an m-message $(q_{\mathcal{V}}, q_{\mathcal{M}})$-space-bounded quantum verifier V for quantum interactive proof systems such that, for every n and for every input x of length n,

(Completeness) if $x \in A_{\mathrm{yes}}$, there exist a function $q_{\mathcal{P}} \colon \mathbb{Z}^+ \to \mathbb{N}$, and an m-message $(q_{\mathcal{M}}, q_{\mathcal{P}})$-space-bounded quantum prover P such that (V, P) accepts x with probability at least $c(n)$,

(Soundness) if $x \in A_{\mathrm{no}}$, for any function $q_{\mathcal{P}}' \colon \mathbb{Z}^+ \to \mathbb{N}$, and any m-message $(q_{\mathcal{M}}, q_{\mathcal{P}}')$-space-bounded quantum prover P', (V, P') accepts x with probability at most $s(n)$.

Next, we introduce the notions of *public-coin* quantum verifiers and *public-coin* quantum interactive proof systems. Intuitively, a quantum verifier for quantum interactive proof systems is public-coin if every message from V consists of a sequence of outcomes of a fair classical coin-flipping.

Formally, an m-message $(q_{\mathcal{V}}, q_{\mathcal{M}})$-space-bounded quantum verifier V for quantum interactive proof systems is *public-coin* if V has the following properties for every n and for every input x of length n. At the jth transformation of V for $1 \le j \le \lfloor m(n)/2 \rfloor$, V first receives at most $q_{\mathcal{M}}(n)$ qubits from a prover, then flips a fair classical coin at most $q_{\mathcal{M}}(n)$ times to generate a random string r_j of length at most $q_{\mathcal{M}}(n)$, and sends r_j to the prover.

An m-message $(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-space-bounded quantum interactive proof system is *public-coin* if the associated m-message $(q_{\mathcal{V}}, q_{\mathcal{M}})$-space-bounded quantum verifier is public-coin.

The class of problems having an m-message public-coin quantum interactive proof system with completeness accepting probability at least c and soundness accepting probability at most s is denoted by $\mathrm{QAM}(m, c, s)$. The following is the formal definition of the class $\mathrm{QAM}(m, c, s)$.

Definition 44. Given a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0, 1]$, a problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ is in $\mathrm{QAM}(m, c, s)$ iff there exist polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ iff there exist polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and an m-message $(q_{\mathcal{V}}, q_{\mathcal{M}})$-space-bounded public-coin quantum verifier V for quantum interactive proof systems such that, for every n and for every input x of length n,

(Completeness) if $x \in A_{\mathrm{yes}}$, there exist a function $q_{\mathcal{P}} \colon \mathbb{Z}^+ \to \mathbb{N}$, and an m-message $(q_{\mathcal{M}}, q_{\mathcal{P}})$-space-bounded quantum prover P such that (V, P) accepts x with probability at least $c(n)$,

(Soundness) if $x \in A_{\mathrm{no}}$, for any function $q_{\mathcal{P}}' \colon \mathbb{Z}^+ \to \mathbb{N}$, and any m-message $(q_{\mathcal{M}}, q_{\mathcal{P}}')$-space-bounded quantum prover P', (V, P') accepts x with probability at most $s(n)$.

B   Note on the Choice of Universal Gate Set

When proving statements concerning quantum perfect zero-knowledge proofs or proofs having perfect complete-ness, we assume that our universal gate set satisfies some conditions, since these "perfect" properties may not hold with an arbitrary universal gate set.

For instance, in the case of the paper by Kitaev and Watrous [20], when we try to implement their parallelization protocol to three messages by *unitary* quantum circuits, we need to implement the controlled-unitary operation controlled by the message index r chosen by the verifier at his first transformation. If this implementation is not exact, we may lose the perfect completeness property after the parallelization, which affects their final statement that any problem in QIP has a three-message quantum interactive proof system of *perfect completeness* with exponentially small error in soundness.

Furthermore, in the case of the paper by Marriott and Watrous [23], their method of converting any three-message quantum interactive proof system to a three-message public-coin one works well only if the original three-message protocol is implemented with *unitary* quantum circuits. Thus, their result inherits the problem of how to implement with unitary circuits the parallelization protocol due to Kitaev and Watrous [20], when claiming their statement in a final form that any problem in QIP has a three-message public-coin quantum interactive proof system of *perfect completeness* with exponentially small error in soundness (i.e., $\text{QIP} \subseteq \text{QMAM}(1, 2^{-p})$ for any polynomially bounded function p).

This is also the case for the present paper, since we are using both a modified version of the parallelization protocol due to Kitaev and Watrous [20] and a public-coin technique due to Marriott and Watrous [23]. In our case, if the implementations of the controlled-unitary transformations are not exact, we may lose the perfect zero-knowledge property after the parallelization, since the implementations used for the simulator may differ from those used for the honest verifier.

One direct solution to avoid these problems is to use such a universal gate set that (i) the Hadamard and Toffoli gates are exactly implementable with a constant number of gates in the universal gate set, and (ii) given a circuit Q consisting of gates in the universal gate set that exactly implements a unitary transformation U, we can construct another circuit Q' consisting of gates in the same universal gate set that exactly implements the controlled-U transformation such that the size of Q' is bounded by polynomial with respect to the size of Q. For instance, if the Toffoli gate is in our universal gate set $\mathfrak{U}$ and the controlled-U gate is necessarily included in $\mathfrak{U}$ for any gate U in $\mathfrak{U}$ not of controlled-unitary type, the condition (ii) is satisfied. This is because the controlled-controlled-U operator is easily realized by the controlled-U and Toffoli gates. From these observations, one can see that, for example, the set consisting of the Hadamard gate, the controlled-Hadamard gate, and the Toffoli gate satisfies both (i) and (ii).

Watrous [35] pointed out that the condition (ii) is actually not necessary for our purpose. In fact, what we need is a unitary implementation of the parallelization protocol that does not lose the "perfect" properties. The essence of the Kitaev-Watrous parallelization method lies in the use of the controlled-swap test. Note that, if we may assume the condition (i), the controlled-swap transformation can be implemented exactly. Now, instead of implementing the controlled-unitary operation controlled by the message index r, we may implement the following that is sufficient for our purpose. For simplicity, it is assumed that r is chosen from the set $\{0, \ldots, 2^l - 1\}$ for some positive integer l (such an assumption does not lose generality because we can appropriately add "dummy" messages to the underlying protocol so that the number of messages becomes 2^{l+1} in the underlying protocol), and the unitary transformation U_r is applied when r is chosen. Suppose U_r acts over q qubits in a register T, for each r. We prepare ancillae of q qubits in a register A_r for each r, and set the control qubits in a register C to the state $\frac{1}{\sqrt{2^l}} \sum_{r=0}^{2^l-1} |r\rangle$. We first swap the content of T and that of A_r when the content of C is r, for each r (this can be realized using controlled-swap transformations). Next we apply $U_0 \otimes \cdots \otimes U_{2^l-1}$ to the qubits in $(\mathsf{A}_0, \ldots, \mathsf{A}_{2^l-1})$, and then we again swap the content of T and that of A_r when the content of C is r, for each r. This results in applying $U_0 \otimes \cdots \otimes U_{r-1} \otimes I_{2^q} \otimes U_{r+1} \otimes \cdots \otimes U_{2^l-1}$ to some meaningless quantum state when the content of C is r, and thus, would not keep the coherence of the quantum state in C. However, recall that the control part in the Kitaev-Watrous parallelization protocol is the message index r, which is originally chosen

at random *classically* when we describe the protocol in a non-unitary manner. Hence such decoherence does not affect the protocol at all, and we can have the unitary implementation of the protocol only using the circuits for U_r's and for the controlled-swap operation. We may also use a similar technique when constructing a simulator. To avoid unnecessary complication, now the honest verifier sends all the ancilla qubits in the registers $\mathsf{A}_0, \ldots, \mathsf{A}_{2^l-1}$ to a prover at the second message in addition to the actual message prescribed in the protocol. The honest prover just ignores these ancilla qubits when sending the third message, and the simulator does not need to simulate the ancilla qubits. Therefore, all the "perfect" properties claimed in this paper (and ones in Refs. [20, 23]) hold with any gate set such that the Hadamard transformation and any classical reversible transformations are exactly implementable. Fortunately, most of the standard gate sets satisfy this condition. A typical example is the Shor basis [30] consisting of the Hadamard gate, the controlled-i-phase-shift gate, and the Toffoli gate.